HOUSE OF LORDS

Select Committee on the Constitution

2nd Report of Session 2008–09

Surveillance: Citizens and the State

Volume II: Evidence

Ordered to be printed 21 January 2009 and published 6 February 2009

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 18–II

CONTENTS

Written Evidence

NOTE: The Report of the Committee is published in Volume I (HL Paper 18-I)
The Evidence of the Committee is published in Volume II (HL Paper 18-II)

Minutes of Evidence

TAKEN BEFORE THE CONSTITUTION COMMITTEE

WEDNESDAY 14 NOVEMBER 2007

Present	Bledisloe, V	Quin, B
	Goodlad, L	Smith of Clifton, L
	Holme of Cheltenham, L (Chairman)	Windlesham, L
	Lyell Markyate, L	Woolf, L
	Morris of Aberavon, L	Rodgers of Quarry Bank, L
	O'Cathain, B	

Memorandum by the Information Commissioner

EXECUTIVE SUMMARY

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000.

2. Concerns about the potential for information technology to compile detailed collections of information about individuals to cross compare this with information from many sources and transfer this elsewhere easily and widely started to raise concerns about the detriment to individuals and the fabric of society as far back as the 1970. Data protection legislation was introduced at national and international level does deal with these concerns. Advances in technology mean that now individuals leave electronic footprints behind in many aspects of their daily lives. This has increased the capability for surveillance of the citizen through data collection.

3. Whilst this extensive use of personal information is largely for benign and beneficial purposes the risk that the details of people's everyday lives may be used in unacceptable and detrimental ways cannot be ignored. The impetus for more details to be recorded and used is not just technological but comes from the political, administrative and commercial worlds.

4. The risks for individuals can range from denial of services through inaccurate data, the consequences of security lapses through to being profiled and treated with suspicion on the basis of the most dubious of information. There are also accompanying risks for society as a whole with the loss of personal autonomy, stigmatisation and the growth of excessive organisational power leading to a climate of fear, suspicion or lack of trust. The risks posed by excessive surveillance using personal information means that data protection legislation is even more essential today than when first enacted in the UK in 1984.

5. The Commissioner commissioned research into whether we are living in a surveillance society and published this as part of an international conference on the issue. The report authors concluded that we are living in a "surveillance society" and that debate and safeguards are needed.

6. The Commissioner believes that properly applied data protection safeguards help prevent the undesirable use of personal information and has a number of initiatives to deal with specific issues. These include a revised CCTV code of practice, information sharing framework code of practice and developing privacy impact assessments for the UK. There is also a need to strengthen his powers to inspect and to make sure he is consulted on policy developments at an early stage.

7. His specific recommendations to the Committee are:

- Mandatory privacy impact assessments by government departments.
- Requirements to have codes of practice in place for proactive information sharing in the public sector.
- Proper consultation with the Commissioner before significant new developments.
- Increased audit and inspection powers for the Commissioner.
- Effective penalties for serious disregard for the requirements of the data protection principles.

The Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective.

The March of Technology

2. In the 1970s concerns grew about the increasing potential for information technology to compile detailed collections of information about individuals, to cross-compare with information from many different sources, and to transfer the collected information elsewhere easily and widely. The potential to cause real detriment to individuals and the fabric of society lead to the development of data protection legislation first by some individual countries and then at international level through the OECD, Council of Europe, and the European Union. Few could have envisaged the growth, ready availability and technological advances that have taken place since the UK's own first generation of data protection law was enacted in 1984. Advances in technology mean that as individuals lead their lives in the 21st century they leave electronic footprints behind with the click of mouse, making a phone call, paying with a payment card, using "joined up" government services or just walking down a street where CCTV is in operation. Our transactions are tracked, our interactions identified and our preferences profiled—all with potential to build up an increasingly detailed and intrusive picture of how each of us lives our life. This has increased the capability for surveillance of the citizen through data collection.

3. Information technology has revolutionised people's lives, improved the quality and efficiency of the services provided to them and has become an essential feature of modern life in the developed world. Individuals can receive quicker, better and a wider range of services from private and public sectors. Technology can and does help improve essential services like health care and provide greater public safety. Many of these technological advances involve increased acquisition of personal information. Whilst this extensive use of personal information is largely for beneficial benign purposes, the risk that details of people's everyday lives may be used in unacceptable, detrimental and intrusive ways cannot be ignored. The State is in a particularly powerful position. This is not just because of the picture it can build up on individuals through the range of services the public sector provides. Through compulsion the State can require not just individuals to provide it with information but also the private sector as it takes powers to require the provision of information such as with sections 9 and 38 of the Identity Cards Act 2006. This raises the potential to change the whole balance of the relationship between the State and its citizens with increased intrusion into their lives.

4. The Commissioner, in discharging his statutory data protection responsibilities, is particularly well placed to view the growth and changes in information handling and the risks these may pose. The developments are not limited to increased technological capability. There is also an increased impetus from the political, administrative and commercial worlds to bring together more and more information. There is an understandable desire to harness technological change to fight terrorism and other crime and to transform public services. The business world can already demonstrate the value of acquiring information about customers, their preferences and their activities.

5. There has hitherto been widespread lack of awareness—and a corresponding lack of public debate—about these developments. There is need for much greater attention, and a higher profile, to be given to the technological capacities, to the nature and extent of information processing, to the risks involved and to the safeguards which are needed. As the pace accelerates, the Commissioner's concern is to ensure that full consideration is given to the impact on individuals and society, that pre-emptive action is taken where necessary to minimise intrusion and that measures are in place to safeguard against unjustified detrimental consequences. The issues are complex, difficult and controversial. The Committee, in its invitation to provide evidence, rightly recognises that questions are now raised about the nature of society, about the role of the state, about the activities of commercial bodies and about the autonomy of citizens. There are no black-and–white solutions but public and political discussion is essential before developments become irreversible, before the risks materialise and before there is a public backlash. The Commissioner has sought to raise awareness and stimulate debate and wholeheartedly welcomes the focus which the Committee's inquiry will now bring.

The Risks

6. The risks that arise as a result of excessive surveillance affect us individually and affect society as a whole. There can be excessive intrusion into people's lives with hidden, unacceptable and detrimental uses. Mistakes can be made and inaccuracies can occur disrupting individuals' everyday lives as increasing reliance is placed on single central collections of personal information running the risk that individuals become frustrated as "the computer says no". Examples are not confined to service provision, "false positives" on foreign government aviation security watch lists have resulted in innocent individuals having their air travel restricted from the UK.

7. Breaches of security can have even more significant consequences. There is a thriving black market in personal details and there are frequent reports of the most personal of details being inadvertently revealed in security lapses. Both these can have serious consequences for individuals putting them at risk of identity fraud. There is also great potential for more discrimination, social sorting and social exclusion as details of individuals are analysed, profiles built up and decisions made on how to treat them. For example moves are already underway to try to identify children who may grow up into one of the 20% of adults who are believed to commit 80% of the crime. This involves analysing circumstantial risk factors such as family members' criminal records. This runs the real risk that children are stigmatised from an early age and however well behaved they may be are treated with suspicion. As developments such as vehicle and mobile phone tracking develop there is the danger that such surveillance fosters suspicion and causes trust to evaporate. For individuals the risk is that they will suffer harm because information about them is:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who ought not to have it;
- used in unacceptable or unexpected ways beyond their control; or
- not kept securely.

For society the wider harm can include:

- excessive intrusion into private life which is widely seen as unacceptable;
- loss of personal autonomy or dignity;
- arbitrary decision-making about individuals, or their stigmatisation or exclusion;
- the growth of excessive organisational power; and
- a climate of fear, suspicion or lack of trust.

The Importance of Data Protection

8. The risks of excessive surveillance by using personal information—and the harm that could be caused if the risks are realised—mean that effective data protection safeguards are even more essential today than when they were first enacted in the UK in 1984. The eight data protection principles that lie at the heart of the Data Protection Act 1998 match closely on to the risks as set out above. Similarly the Data Protection Act plays a valuable role in helping address actual and potential interferences with Article 8 of the European Convention on Human Rights by focussing safeguards aimed at securing appropriate privacy in respect of personal information.

9. The role of the Information Commissioner under data protection law involves the promotion of good practice, guidance to organisations, advice to the public, enforcement action where the law is broken and the resolution of complaints. These responsibilities—especially in proactively encouraging compliance—are vital as individuals are increasingly affected by the greater and ever more detailed collection of information about them and the wider uses to which this is put in practice. The Commissioner is aware that data protection requirements have sometimes been seen as technical, bureaucratic impositions. To reverse such attitudes the Commissioner's overall strategic approach to his data protection responsibilities is now aimed at "Strengthening public confidence in data protection by taking a practical, down to earth approach—simplifying and making it easier for the majority of organisations who seek to handle personal information well and tougher for the minority who do not". To achieve this the Information Commissioner's Office (ICO) takes a risk based approach, focussing attention and resources where there is a real risk of harm and where its interventions are most likely to make a difference both in the short and long term.

A Surveillance Society?

10. The Commissioner used his role as host of the 28th International Conference of Data Protection and Privacy Commissioners in November 2006 to focus debate on whether we are now living in what may be described as "the surveillance society". The centre piece of discussion was a specially commissioned report from the Surveillance Studies Network to detail the extent and facets of surveillance and suggest any areas of particular concern or future action. The report has been updated to take account of the discussions at the Conference and a copy provided to the Committee with this evidence. It is an extensive and thorough report with expert analysis on how surveillance has grown in often benign ways, pointing out the challenges for the future. It is unnecessary to reiterate the contents of the report in this evidence but the Commissioner welcomes the detailed research and general thrust of the report as a thorough analysis on which to base his own approach to the issues. He commends the report to the Committee as a comprehensive and reliable analysis to help inform its own deliberations. It is an account that makes clear that the challenges we face in ensuring existing and future developments inspire public confidence are not ones limited to data protection and privacy. The challenges extend to other factors such as the risk of social sorting and exclusion which also affect the fabric of the society in which we live and the relationship between citizens and the State. The report refers to contributions to the International Conference and how following the downfall of totalitarian states there still remain dilemmas of privacy, trust and social relationships.

11. The Commissioner does not believe that we in the UK are living in a surveillance society of the type that is associated with totalitarian regimes—of the past, the present and potentially the future. Political commitment to the imperatives of a stable, democratic and consensual society—and the associated checks and balances—will always provide much stronger safeguards against any risk of totalitarianism than can be provided through strong data protection or similar controls.

12. The Network's report adopted a somewhat broader approach to the meaning of surveillance when talking about a "surveillance society".

> "Where we find purposeful routine, systematic and focussed attention paid to personal details for the sake of control, entitlement, management, influence or protection, we are looking at surveillance".

13. The report concluded that that we are living in a "surveillance society" within the terms of this definition. The picture described in that report has grown up not for malign reasons but through the cumulative effect of separate developments that have taken place for apparently benign purposes. The report serves as a "wake-up call" on the dangers that can come with surveillance if it is not accompanied by vigorous debate and political consensus about where lines should be drawn and about the restrictions and safeguards which are needed.

The ICO Approach

14. The Commissioner believes that properly applied data protection safeguards act as a significant bulwark against the unwarranted and undesirable use of personal information. His strategic approach to surveillance issues is founded on the need to ensure that as relevant developments occur in future data protection and privacy interests are considered at the very earliest stage. It is imperative that these important considerations are taken into account, addressed and built in as developments progress and not ignored or "bolted on" as an afterthought. The Commissioner remains keen to foster public awareness and debate but is committed to providing more tangible assistance towards securing effective data protection and privacy safeguards and inspiring public confidence. To this end he has drawn up a Surveillance Society Action Plan which identifies actual activities that he can perform within his existing statutory powers.

15. The key points in the Action Plan fall into two work streams: awareness-raising and practical measures. The ICO will maintain awareness-raising activities following the publication of the Surveillance Society Report for example by commissioning new research into public attitudes to surveillance. The ICO will also embark on a series of practical measures. Some of this work involves ensuring that existing developments that have a surveillance society dimension move forward in a way that recognises and takes account of legitimate data protection and privacy concerns. Examples include the issuing of ID Cards and creation of the National Identity Register, the acquisition of powers by government to gain access to private sector data, plans for road user charging/vehicle tracking and the development of e-Borders.

16. Other proactive tools and approaches are also being developed by the Commissioner. These are designed to realise the aim that data protection and privacy issues are identified and addressed at the outset and safeguards built into systems of work. The ICO is developing an Information Sharing Framework Code of Practice to help ensure that the Government's vision of transforming public services through increased information sharing develops in a manner consistent with data protection requirements. The Commissioner's

CCTV Code of Practice is also being updated to take account of the massive growth of CCTV surveillance in the UK and changes in methods of operation and technology that have taken place since it was first published in 2000. Both these codes of practice will be published during the coming year after full consultation. In addition the Commissioner is now discussing with the Cabinet Office its information assurance initiatives which should help ensure proper security and reliability of personal information.

Privacy Enhancing Technologies

17. The Commissioner is also concerned that best use is made of what may be described as "privacy enhancing technologies". This involves using technology itself to minimise data collection and provide intrinsic safeguards. The Royal Academy of Engineering in its report "Dilemmas of Privacy and Surveillance: Challenges of Technological Change" also advocates exploiting engineering ingenuity to protect privacy. One area that is particularly interesting is identity management and the opportunities technologies provide to minimise the identifying particulars needed to provide services, thereby reducing the associated data protection risk. The Austrian Government in its provision of e-government services employs the use of "fractional personal identification numbers" which allows relevant information in different collections of information to be accessed without the need for a single widely known personal identification number that may be misused. The ICO is sponsoring a strategy forum at the Oxford Internet Institute (7 & 8 June 2007) that will examine new and potentially more privacy friendly ways of achieving effective identity management to the advantage of service providers and individuals alike.

Privacy Impact Assessments

18. One of the most significant new initiatives is based on privacy impact assessments. Privacy impact assessments are commonly used in other countries, most notably Australia, Canada, New Zealand and the USA. In the USA, the E-Government Act 2002 requires that a privacy impact assessment is undertaken and published before the government develops a new information system or initiates a new collection of personally identifiable information. Such impact assessments are based on assessing a proposed development by gauging the likely privacy impact on those whose data may be collected and identifying more privacy friendly ways for the same objectives to be achieved. One of the significant benefits of the assessment process is that this takes place during the development of proposals when there is still an opportunity to influence the proposal. Furthermore it can be undertaken by a third party thereby providing a degree of external validation.

19. The aim of the ICO's work on privacy impact assessments is to provide a practical tool that can be used to help shape developments. There is a danger that a privacy impact assessment might be viewed as a further, unwelcome bureaucratic procedure. This would be a mistake. The privacy impact assessment is an aid to designing and implementing privacy friendly ways of working. They help inspire public's confidence in how their information will be handled. To this end the ICO is commissioning an external project to develop the concept of privacy impact assessments for the UK market. This will include provision of a privacy assessment handbook for use by practitioners. An invitation to tender has been issued and it is intended that this work will be completed by November 2007. The Department for Transport has made a welcome offer to assist the selected contractor by allowing its plans for road user charging to be used to provide a practical basis for this research.

20. The Commissioner is regularly frustrated when policy developments in central government proceed a long way before he is called upon to express a view, if he is at all. Although the situation has improved recently consideration could be given to a more formal requirement on government and the wider public sector to seek the Commissioner's opinion on particular types of developments at an early stage. It is possible that such a requirement could be incorporated into the privacy impact assessment procedure. A recent example of where a bill was introduced to Parliament but data protection safeguards only incorporated during the passage of the legislation is the Serious Crime Bill. Amendments were introduced during its passage through the House of Lords to require compliance by specified anti-fraud organisations with a code of practice and that the Information Commissioner must be consulted on the provisions of the code. Whilst such amendments and the continued vigilance of our legislators is welcome, it is regrettable that these privacy safeguards were not on the face of the bill when it entered the Parliamentary process.

Powers

21. Although the Commissioner can undertake a number of actions using his existing powers, the challenges arising from the risks of a surveillance society highlight deficiencies in these powers. The Commissioner has a power to conduct audit and inspections to ensure compliance but this is fettered by a requirement to have

the consent of the data controller concerned. This limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance. There are also limitations to the sanctions that may be imposed where data protection principles are breached. Whilst the Commissioner has the power to issue enforcement notices, these are remedial in effect and do not impose any element of punishment for wrong doing. Such an approach may be appropriate for isolated contraventions of the law or where there is a genuine misunderstanding but a more effective sanction is needed where there are flagrant far reaching breaches of the law. This is particularly true where significant security breaches occur because of the negligence or recklessness of the data controller.

22. Improvements to the Commissioner's powers to undertake proactive audits and the introduction of a penalty for flagrant breaches of the Data Protection Act would send a strong signal that compliance with the law is not just for the virtuous but needs to be taken seriously by all.

23. The Commissioner believes that data protection legislation and his own office both have a vital role to play in addressing the risks that accompany our surveillance society. However, he does recognise that some of the societal effects fall outside his direct competence and that must beg the question of whether some wider form of oversight is now appropriate.

Issues

24. In conclusion the Commissioner believes that the risks of excessive surveillance are with us today. Different types of surveillance activity have not grown up in a malign way and many aspects are essential and beneficial features of modern life. However, the risks to individuals and society are evident and positive action is required to ensure that these risks do not manifest themselves and that unwarranted harm does not occur. Otherwise the trust and confidence which the public must have in all organisations that hold information about them will be placed in jeopardy. Similarly the relationship between the State and its citizens may alter as the chilling effect of greater and greater surveillance is felt by individuals and society as a whole.

25. The Commissioner proposes that the Committee gives particular consideration to the following measures:

- Mandatory privacy impact assessments by government departments.
- Requirements to have codes of practice in place for proactive information sharing in the public sector.
- Proper consultation with the Commissioner before significant new developments.
- Increased audit and inspection powers for the Commissioner.
- Effective penalties for serious disregard for the requirements of the data protection principles.

7 June 2007

Examination of Witnesses

Witnesses: Mr Richard Thomas, Information Commissioner, Mr David Smith, Deputy Commissioner and Mr Jonathan Bamford, Assistant Commissioner, examined.

Q1 ***Chairman:*** Mr Thomas, welcome. We are very glad to see you here. Would you be kind enough to identify your colleagues?
Mr Thomas: Thank you, my Lord. On my right is David Smith, who is my Deputy Information Commissioner and on my left is Jonathan Bamford, who is the Assistant Commissioner with particular responsibilities in this area.

Q2 ***Chairman:*** Your appearance before us is really the first substantive evidence we have had in the new inquiry on which we are embarking, and we are delighted to have you here. In fact I can say that your own writing and speaking about the surveillance society has been part of the inspiration for our work. Is there something by way of an opening statement that you would like to say to us?
Mr Thomas: Thank you very much, my Lord. We are delighted to be here this morning. We are very pleased that this Committee has launched this inquiry. We have submitted written evidence to the Committee and I hope that this morning we can highlight and elaborate some of the points in our written submission to the Committee. I think you are aware of—and we have provided to you—the report that we published this time last year, November 2006, which we commissioned from the Surveillance Studies Network for a conference we held in London, and that elaborated the situation as it was in 2006 and also rolled forward to what life might look like in the year 2016. The nature and the extent of surveillance involving the collection and processing of vast amounts of information about our private lives does raise some fundamental constitutional issues about

the nature of society, about liberties, freedoms and human rights, about the autonomy of citizens, about the role of the state and about the relationship between state and citizen. Surveillance is perhaps traditionally associated with totalitarian regimes but some of the risks can arise within a more democratic framework. Our role has been primarily to raise awareness and stimulate debate. We wholeheartedly welcome the focus which this inquiry will bring on the issues and I think it is part of a general raising of awareness which has been going on perhaps over the last 12 months, about which we are very pleased, because before then there had been a quite substantial lack of awareness and a corresponding lack of public debate about many technological, governmental, policing and commercial developments. We think there is need for much greater attention to be focused on the risks involved and the safeguards which are needed. We all now leave our electronic footprints in many places on a daily basis and as the pace accelerates our concern is to ensure that full consideration is given to the impact on individuals and society, that pre-emptive action is taken where necessary to minimise intrusion, and that measures are in place to safeguard against unacceptable consequences. The issues certainly, we think, are complex and controversial—there are no black and white or easy solutions—but we think that the more debate and discussion before some developments become irreversible, before the risks materialise and before there is a public backlash is very important. We are very keen to emphasise that certainly we are not suggesting that any sort of surveillance society is developing for malign reasons; it is more the cumulative effect of separate developments with benign and well-intentioned purposes. We believe that the report we published last year served as a wake-up call on the various dangers that can arise in this area. We believe that there are risks and there are dangers which can result from excessive surveillance, and this can be divided very broadly into those which impact negatively and sometimes very seriously on individuals and those affecting society as a whole. Both types of detriment can arise from mistakes, from inaccurate or outdated information, from security breaches, from excessive intrusion, from the hidden collection of information and from the unacceptable use of information. The risks grow as ever increasing reliance is placed on single or centralised collections of personal information. We are very pleased, Chairman, that the debate has now broadened; there are not many subjects where the *Daily Mail* and the *Guardian* can both unite on these sorts of issues with the coverage they have been giving to them over the last year, but also there have been some very thoughtful articles quite recently, for example, in *The Economist* and in *The Sunday Times*, which have given a very full analysis of the various issues, and we are pleased to see that level of debate going on.

Q3 ***Chairman:*** Thank you very much. You have touched on a number of the issues which will concern the Committee, but can I start by saying something that has come very clearly to our attention, even in these very early days of deliberation, which is the difficulty of getting any 360 degree review of these issues. Even in the evidence given to us by the Ministry of Justice we find the lack of any overarching 360 degree context; there seems to be no general principles nor a firm legal basis, nor a whole-of-government view across departments, or for that matter an overarching regulatory framework. We are dealing with an area growing like Topsy—very fast—and driven by change, both social and technological change, and I think one of the problems that the Committee has already had is to try and get our mind around it as a whole, and I would be grateful before we get into some of the detailed questions if you could give your reaction to the partial and sporadic growth of public policy and law in this area and what your reaction is?

Mr Thomas: I think, Chairman, we would very much agree with that sort of analysis. I think it is fair to say that there has not been a single point of reference for all these various developments. The work that we have done has ranged widely; it has drawn attention to very many fragmented developments across both public and private sectors and within government where virtually every government department is involved in one way or another in issues which impact on this subject matter. The Ministry of Justice is a focal point for data protection but the Home Office, the Department for Transport, the Department for Children and Schools, the Department of Health, all in their various ways have an interest and are doing work which has a bearing on the issues with which we are concerned. I think there are signs of a sea change; I think the Prime Minister's speech on Liberty on 25 October, which devoted some five pages to looking at privacy and data protection issues, was the first time I think in living memory that a Prime Minister has addressed these issues so fully and already there are signs that that is sending out signals across Whitehall that the protections and safeguards must be taken very much more seriously. Over recent years perhaps there has been a push to gather more and more information, to harness the benefits of technology without perhaps giving thought both at the fragmented level and at the general level as to some of the implications, some of the safeguards needed. Your final point perhaps was about the regulatory framework. I think we would say that the Data Protection Act, the legislation on the data protection, does provide a broad, horizontal framework and although I and others have some reservations about

some of the detail of the legislation, the fundamental principles which lie at the heart of this in the European Directive and at the heart of the 1998 UK Act I think have broadly stood the test of time. I think they do address the sort of safeguards that we need to have in place and we can elaborate this morning as to how we are trying to apply those in practice. So I think the principles are sound and I think they do provide a good reference point for judging what is acceptable and what is not acceptable, but perhaps some of the machinery for implementing that is getting a bit creaky now and we might look at ways to improve that.

Q4 ***Chairman:*** I am sure we will come back to that in the course of the questioning. One thing that the Committee has become aware of in preparing for this inquiry is what is called profiling, where a set of people in society are created through shared data characteristics which then potentially determines public or penal or other policy towards them. Since a lot of the emphasis is on the individual I wondered whether you could talk about the indications of profiling as a guide to policy approaches in a number of areas and any dangers of which you are aware.

Mr Thomas: Perhaps I could start on that and then ask one of my colleagues to take the issue a bit further. Perhaps in some way the starting point is what has happened in the private sector. Everybody in this room will be aware now of how sophisticated marketing has become in recent years—holiday companies know where you are likely to want to go on holiday, Amazon will know your reading habits. The private sector has become very sophisticated, using a lot of commercial information, postcode information and so on to really build up a picture about our preferences and our experiences. I think the public sector is, if you like, catching up in this area. The police are enthusiastic about profiling and one can see perfectly legitimate uses of profiling when they are trying to deal with particular types of criminal behaviour and I do not think anybody would have any difficulty with that where it is done properly. Likewise, profiling is now being talked about more and more in the area of child welfare, child protection, in the health area and so on. In principle targeting people so that we know what the issues are in the public sector, with which we are dealing, is a good thing and we are keen to emphasise that. But there are dangers. I can give you one example: we know that some 20 per cent of adults commit 80 per cent of crimes but does that justify looking at children as they are growing up, looking at the criminal records of their parents, looking at the social circumstances of their household to say, "That is a likely criminal for the future who needs particular watching in the classroom or in the local community". An even more acute example is that there is evidence to correlate the link between victims of child and sexual abuse and those who later in life become sexual abusers themselves. Does that justify taking a profile of victims of sexual abuse and saying, "We have to watch these people very closely because they may be the offenders of the future?" There are other examples which my colleague might share with the Committee.

Mr Bamford: Building on what the Commissioner has said, we see many aspects of risk assessment in administrative life. When you have stretched resources, when you have particular problems you focus on risk and look for risk areas, and that is the area where profiling comes into its own really; it is trying to use information to direct your resources and your interests into particular areas. I tend to use the example of the children who are going to grow up to be the 20 per cent of adults who commit 80 per cent of the crime then we end up with the situation of that activity generating lots and lots of information. So you see that there is more and more information being utilised to try and tease out these risk factors. When you are working with a degree of certainty maybe that is not a bad approach but when you start to deal with some more nebulous matters that becomes a bit more difficult, so the criteria to generate the risk is flawed in some way. So we see dealing with risk generates profiling; we see it in the public sector and we see it in the private sector. You could say it may be more in the private sector for profiling customers for good things; in the public sector we often see it for things which have a detrimental effect on individuals—whether a person should be allowed on to an aircraft or not because they happen to share some characteristics with somebody deemed as a risk.

Mr Thomas: I think there is a wider debate and this is covered very fully in the report that we have published, that the more you use profiling the more you run the risk of going down a society where there is greater stigmatisation, more discrimination, more social exclusion and a society of greater suspicion where trust is reduced.

Chairman: Where the data becomes predictive, if I can extend the example you both hinted at, I think I am right in saying that if you are a special needs child in a school you have about a three times higher probability of being excluded from school than the average child. Then we learn that children excluded from school have about a three times greater likelihood of subsequently becoming offenders. So it is quite a skip and a jump from a child having special needs at school to saying that such a child has a nine times higher probability of offending than the average child, and it then becomes a predictor of policy. I think Baroness Quin has a question.

Baroness Quin: It is certainly an area about which I am concerned as well in terms of the fact that it might blight someone's chances of employment and getting

opportunities in life afterwards, and I wondered if you felt that there was a bit of a problem between the need to try and protect society from risk and yet the principle of believing in rehabilitation? If someone has served a sentence then they have paid their dues to society and should not be penalised for the rest of their lives.

Chairman: I am going to take Lord Bledisloe who has a question on this point as well.

Q5 ***Viscount Bledisloe:*** Taking, for example, these children that you refer to in your paragraph 7, the ones whose fathers were thought to be regular burglars or, indeed, the ones who are thought to have been victims of abuse, surely at the very minimum they must be told that they are on a register because of that because they may want to say either, "He was not my father," or "But he moved out of home when I was one and had nothing to do with me", or he may want to say, "You have got it wrong."

Mr Smith: There is a very good example, Chairman, both of stigmatising and of competing public policy objectives in the checks that are made on people who want to work with children, particularly criminal records checks; and it goes more than into the criminal record, it is actually that any information held by the police can come out in a check. We had a system which was inadequate; it allowed people to work with children who were not subject to proper checks. But in addressing that public policy concern we have gone very much the other way, so that if I applied now for a job to work with children any conviction that I have ever had would be revealed to my potential employers, whether or not it had any bearing at all on my risk to children. So the fact that I was convicted of shoplifting as a teenager, which was unfortunate and I regret it and I have put it behind me, will come out. If that employer refuses me the job I will think it is was because of that conviction whether it is the case or it is not. I will think that I have been prejudiced against. I have no doubt that in the risk averse climate we have with child protection with any speck that is there employers will say, "No, we will leave that person alone, we will go for someone else." So I think that is a very good example. The other example, which is slightly different, is to do with airlines and airline passengers where there is a profiling arrangement—people present risk factors. One of the problems that you see, particularly when people go to the States, is that the same people keep getting stopped. They may present under the profile at one time, they get stopped, they get questioned, but then there is not the information management processes to update the profile so the next time the record says, "No, this person may present but do not stop them." It is about proper information management processes to go alongside the increased collection and use of information.

Q6 ***Chairman:*** I think the links you have all made between over-zealous risk management and surveillance is a very important one. Thank you for that. Can I move on and ask you, in terms of the plethora of current and proposed policy initiatives with which we are faced, are there any that you as Information Commissioner see as posing a particular threat either to the privacy of the individual or the well being of society?

Mr Thomas: Perhaps I could give you a list of current initiatives which I think have a bearing on this and we can develop that? I think the identity card debate and the national identity register, the database behind that is an area that has been of particular concern to us. The e-borders programme; Connecting for Health, the National Health Service project to have full electronic health records in due course on every person in this country; the road user charging possibility if we have intrusive means of tracking vehicles as they are driving around the country; the Serious Crime Act which has just very recently received Royal Assent is an example of authorising public sector access to private sector databases in the fight against fraud; the new rules recently brought forward for the retention of telecoms details by telephone companies with access to that by the police. Those are just some examples and we can say more about any of those as you choose.

Q7 ***Chairman:*** All of those, their proponents will claim, have social and other benefits. Of the ones you have identified—and it is a very helpful list—are there any where to you, as the Information Commissioner, the negatives clearly outweigh the positives?

Mr Thomas: We are very conscious that we are appointees; we are not a democratic institution, and so when Parliament decides that there should be an identity card system we respect the will of Parliament on that. At the same time we are aware of the controversy as that was going through Parliament. We engage with the Passport and Identity Agency, and indeed we have a meeting this afternoon to look for how that is going to work in practice, to try and minimise the risks to citizens. We have always made it clear that one of our major concerns has been the database—it is not so much the cards it is the database behind the cards—and we continue to question why so much transaction data is going to be collected. It is one thing to have a card to prove your identity but why do we have to have a record on that database every time the card is swiped through a terminal, whether at Heathrow, at a police station, at a social security office or wherever? We have questions about the database of all children that is being put together in this country, every child from birth until 18 years old. We can fully understand the rationale for collecting information about children

who are at risk of physical or mental abuse or other forms of unacceptable treatment from their parents or their guardians; no one, I think, would quarrel with the need for social services, the police, and the schools to at least be aware of the children who are at particular risk. But we are more sceptical about the need to keep even basic information on all children with the rather more vague purpose of safeguarding their educational development, their health and their social circumstances. I think that is an example where we still have some reservations about a particular database.

Q8 ***Lord Goodlad:*** Commissioner, you mentioned the Prime Minister's recent speech on Liberty in which he mentioned the importance of parliamentary scrutiny of legislation and the granting of powers involving the collection and use of personal data. It would be of great interest to the Committee if you could say how well, in your view, Parliament has been fulfilling this role and what, if anything, you think could be done to increase the effectiveness of parliamentary scrutiny?

Mr Thomas: Thank you, Lord Goodlad. I have mentioned the Prime Minister's speech and I am certainly not making a party point. I thought it was a thoughtful speech on the subject of liberties and I thought there were some very welcome words there about recognising the need for balance in this area. The Prime Minister talks about the need for security against terrorism, the fight against serious crime and fraud; he talks about the improvement of public services. He recognises the benefits of collecting information but he is also very, very clear about the risks. He talks about accountability where people's data is concerned and that government needs to be held, he said, independently to account and that we risk losing people's trust, which is fundamental on all these issues. So I very much welcome what was said in that speech. In terms of parliamentary scrutiny I think it is hugely important that Parliament is vigilant, if I can be so bold, to scrutinise measures as they come forward, and perhaps there has not always been as much scrutiny as I would like to see. In 2003 the legislation was changed to allow the expansion of the national DNA database and that now allows DNA to be retained indefinitely on anybody who is coming to the attention of the police because of any recordable offence, even though they are not prosecuted. Even though they are not convicted the general rule now is that the DNA profile is retained indefinitely. There was not very much debate about that in Parliament. I fully recognise that technology has moved on and perhaps when that was being debated it was quite expensive to obtain DNA profiles. But now technology, even in the last five years or so, has made it much easier to obtain and retain DNA. We are now in the situation where I think probably there are more DNA profiles on the national database than anybody would have contemplated when that was going through. So I think the more the better that Parliament is looking both at primary legislation, which creates the framework, but also at the detail of the secondary legislation—often the devil can be in the detail. I have mentioned our meeting this afternoon where we are going to be discussing the secondary legislation associated with the Identity Card Act and I think it is important there should be as much debate as possible—certainly in Parliament but elsewhere as well, and I am sure that Parliament would not claim any sort of monopoly of scrutiny, and we ourselves have a very important role in trying to alert people to some of the issues. There have been occasions where the parliamentary process has improved the quality of legislation. The Serious Crime Act, which received Royal Assent, was significantly improved on a cross-party basis as the Bill was going through the House of Lords. The new provisions there, which were taken as amendments, were modified slightly in the House of Commons, which essentially say that there should now be a statutory code of practice to govern the public sector access to private sector databases; that there should be a code of practice which should be put together in consultation with myself and that I, as part of that code, should have the right to go and inspect how these arrangements are working in practice. It is not just the codes and the fine words in the codes; it is how they are working in practice. Although we do not have a right under the statute, which I hope we might come on to later—we have no legal right—we now have, if you like, in that particular example, as a result of the parliamentary intervention a quasi contractual right under the code of practice that we can go in to inspect. That is a very good example of Parliament increasing the safeguards in place.

Mr Smith: Could I perhaps put in there a plug for our position because we have a power to report to Parliament, which we have used very occasionally—and we will refer to that later—but where bills are subject to parliamentary scrutiny we are very happy to come and give evidence to the relevant parliamentary committees, and we do that. But it is rather haphazard as to whether we get invited, whether there is investigation of our areas. We wonder whether there is some scope to formalise that arrangement whereby we have a right to be heard or something of that sort in the process where there are significant implications in legislation for the use and collection of personal information.

Q9 ***Chairman:*** It is possible that Parliament would like to find some way of knowing on an Information Commission radar that *prima facie* you think this

raises an information issue that might be worth thinking about.

Mr Thomas: We are not seeking to expand our empire, Chairman, I assure you, but equally our counterparts in other countries do have that sort of function and we think that perhaps the time has come for a little more formalisation of that. It is not just the parliamentary stage, I think we all know that it is at the early stages of policy development and on some occasions government departments have moved forward two or three years without involving us and by that time things get rather set in concrete and it is too late to go back several stages.

Q10 ***Lord Morris of Aberavon:*** Questions were asked in the House of Lords regarding the extension of DNA and I do not think we pinpointed sufficiently the fact that there would be millions and millions—and in due course possibly all of us—on this register. In the old days fingerprints of an accused person, if acquitted, were destroyed. Now "coming to the attention of the police" were the words that you used, everyone is going to remain on this. Did you at the time say anything? Should you have said something? I think I gather from what you have just said that there should be machinery for you to say something to express any concern that you might have?

Mr Thomas: I started at the beginning of 2003 and perhaps we missed a trick in not shouting loud enough. I think we did put in a paper on the subject but perhaps it was not very well publicised and perhaps did not really have the force that it might have had, so I think we recognise, moving forward, that we need to put our views as forcefully as possible. But these are difficult issues. On the DNA database we fully recognise its functions—there has been a case this week where a conviction has been secured many, many years after the event and I think everybody would welcome that. But we would question, for example, if, as a citizen who does not have a conviction and your sample is taken and it is run against the database of samples taken at scenes of crime, if you are clear—why does that sample have to be kept indefinitely? It is one thing to take a sample and apply it on the spot, as it were—maybe it takes seven days—but why should that be kept on an indefinite basis? What we are also saying, going back to the Chairman's opening comment, is that there are so many developments across so many aspects of public life now that I think we could not undertake to get involved in every single one; what we would like to do is to have a stronger right to come forward—either the law requires some consultation with our office or that there is a duty when a new scheme is being introduced to consult with us. I would like to say more later about privacy impact assessments because I think that is a technique for addressing some of the issues as schemes come forward, but I think there are various techniques to give us a more formal involvement.

Q11 ***Baroness O'Cathain:*** I am going to take a rather different view actually. I feel rather comforted by a lot of the information that is collected on me and I also believe that longer term having the DNA of everybody in this country might not be a bad idea because there are huge benefits in having it, at least those people who are most likely to commit crime. I think we are terrified of this whole criminal side of it. A very simple example of the positive benefit of data collection, which I made when we were talking about this. When you go to license your car you can actually do it in two minutes and not take your MOT and not take your registration book and not do anything else. I have to tell you that that is a great advantage as all data is shared between DVLA and the Department for Transport. Secondly, if you are involved in an accident and if, for example, your DNA was on a register they might say, "This is a person . . ."—and because relevant health data is stored—". . . for goodness sake do not give them penicillin otherwise they will be really dead." I feel that the more information that is held centrally on me the more I am comforted, and secure. But that of course then raises the question of what hands does it get into? But before we get to the point—and I would like your view on this—you made the point that everybody knows so much about us—and again we have spoken about the Tesco syndrome where they literally will not give you special offers on alcohol if they know perfectly well that you never drink because you never buy your alcohol there. They have literally built up a profile on you—it does mean that you get a lot less junk mail. The third point is that we still have—and is this going to continue—a situation where if you subscribe to magazines they ask you your profile or if you do something like buying electrical equipment, to get your guarantee you have to say what other electrical equipment you have had from this organisation. So all of that is happening, but they always do state in a little box at the bottom saying, "We can share this; do you object to sharing this information?" That, of course is a commercial issue, because they sell it. So I just wonder if we are getting too worried about the subjective nature of the way the data is collected and would it not be better to have everybody on the same database?

Mr Thomas: There is a lot of ground in the various points you have made. DVLA I think is a very good example where thought was given for putting in place an arrangement which is undoubtedly of huge benefit to the citizen—two minutes to go on line to renew your car tax rather than two hours queuing at the post office. But on that occasion the arrangements behind the scenes between DVLA, between the

agency which looks after MOT certificates and between the private insurance companies are very important to make sure that that can happen and that the consent of the motorist is secured at the point they use the service. So it is done in a very structured way and I applaud that particular example. I think the debate about a compulsory DNA database for every citizen is a very big debate. Lord Justice Sedley came forward with something similar himself a couple of months ago. I did have some very strong reservations about that and I would be happy to elaborate on that if you would like me to. I think both for practical and civil liberties reasons I am really quite sceptical about the logic of saying that there are some unfair discriminations there at the moment and therefore we resolve that by having everyone's data on a mandatory basis. I would just differ on that point. Your reference to Tesco and to the private sector brings out one of the fundamental points. Nobody forces you to shop at Tesco—you have a choice, you can go to Sainsbury's you can go to Marks & Spencer or wherever and they all have a very strong interest in making sure that they treat your information properly. They safeguard your information as a very, very valuable commercial asset, so they have a self-interest in safeguarding it but also a reputational issue, and in fact all the evidence that we have is that they take a lot of effort to make sure that it is kept safely. But in other areas of life, when you are dealing with social services, with the police, with the tax people, with immigration you do not have the same element of choice and I think that perhaps brings us into the arena of this Committee, the constitutional issues where, at the very least, there needs to be a great deal more transparency—picking up Lord Bledisloe's point earlier about people needing to know where that information is held on them and what information is held. That is one of the very important principles of data protection, being entitled in most cases to see what is held about you. But it also brings us to the situation that if these developments are to take place there needs to be a great deal more public debate. So many of these have happened away from any real parliamentary or public debate or scrutiny; it is only in the last year or so that we have had these questions coming up on radio shows, on television programmes, and I think now people are beginning to wake up to some of the implications.

Q12 ***Baroness Quin:*** Just on a supplementary to that, where in your role do you have the responsibility to try and widen the debate? You did say that you were delighted to see an article in the *Mail* and in the *Guardian*. Do you have the sort of Information Commissioner's PR as the judges do to do the right thing?

Mr Thomas: Yes, I have a statutory duty to promote good practice and there is no question but that part of that is raising public concern. I have a press office and we both proactively and reactively deal with the issues in the media as they come forward.

Q13 ***Viscount Bledisloe:*** Before I come to my question can I ask you one thing arising out of the point you made about my earlier point? Is it sufficient merely to say that you should have a right to ask whether you do have information about me on this because supposing I never was abused as a child, and I did not realise they thought I was in danger, should I not actually be told in advance that there is this information about me rather than asking the question to which I think I know the answer?
Mr Thomas: David, I am sure, will say more about this. I will try and simplify the Data Protection Act in one sentence, which is that very generally you should either agree to or be told about the collection of information and then you are entitled to ask for the full details. So, as a broad proposition, where information is being collected you should know about it—not in all situations, there are some exceptions—but the right I mentioned is the right to see the detail, the actual file with the full details. David may want to say something.
Mr Smith: I was going to give an example where we did have a case which involved the Metropolitan Police, where again it was to do with applying to work with children and the first that someone found out that a complaint had been made about them was when it came out on the report when a check was made when they applied to work with children. We took the view that the Metropolitan Police should have told that person actively that the information was recorded. They came back and said, "But if every time we receive a complaint we have to go and tell everybody that is a huge amount of work," and essentially the position we took was, "You do not have to tell anybody if it is just routine, kept in your records, a piece of your intelligence, but if you are actually going to use that and it is going to appear to be to the potential detriment to that person then you do have an obligation to actively tell them so that they know and they can challenge it if they think it is wrong."
Chairman: That is very clear, thank you.

Q14 ***Viscount Bledisloe:*** Can I come back to my proper question? You quite understandably think that your influence on the formation of government policy before it gets to Parliament should be increased. How do you think that should be done? For example, do you think you should have a statutory consultative role? And do you think that you have power, if you do not have it already, to report to Parliament if you make an objection which

is ignored or overruled? And do you have the resources to cope with that if those powers were given to you?

Mr Thomas: We are very proud of our independence. It is a requirement of the European Directive that there should be an independent supervisory authority and I think it is very important that we are independent. But sometimes being independent has some drawbacks in that you can be out of the Whitehall loop and sometimes in the past—although I think things are changing—we have only come across things too late, as I mentioned earlier, and we have not been consulted to the extent that we perhaps think we ought to have been, and some departments themselves, I think, have recognised rather late in the day that they should have been in touch with us at an earlier stage. Things are moving forward; we have already touched on the possibilities of a statutory duty to consult outside generally or in particular situations. It could be done by some sort of amendment to the Data Protection Act giving a more general right to be consulted. It could be done on each Bill as it comes forward, on a case by case basis—I think there are options there. If the Committee would like we would be happy to write a paper and set out some more detailed suggestions. I do not think we are tied to a particular way forward.

Q15 ***Chairman:*** That would be very helpful.

Mr Thomas: We would be happy to do that. We do have the right to make a special report to Parliament—I forget the exact language, it is Section 52: "The Commissioner shall lay an annual report", which we do every year "before Parliament. But the Commissioner may, from time to time, lay before Parliament such other reports with respect to his functions as he thinks fit." We did that for the first time ever last year and I think perhaps with hindsight it should have been used more frequently. We produced a report called *What Price Privacy?* documenting the pernicious trade in illegal obtaining of personal information, and we may want to have another question on that later. That was an example of using, for the first time ever, that power to lay a report before Parliament, and we did it with a follow-up report six months later documenting what had happened. You also touched on resources and you will not be surprised if I say that our resources are very limited and we cannot, I am afraid, churn out reports like that on too frequent a basis—we have to be quite selective in issues that we address. Equally, if we are to make reports to Parliament the more attention that such a report receives the more (obviously) we would welcome that.

Chairman: We have a lot of questions to ask you so we must crack on. Lord Morris has two questions.

Q16 ***Lord Morris of Aberavon:*** The Prime Minister's recent speech in October discussed privacy protection and other values that might conflict with it, and he charged you and Mark Walport with the task of reviewing the framework for the use of the information and "to assess whether it is right for today's landscape and strikes the right balance". How do you view the terms and scope of this remit, and how do you propose to undertake this assessment?

Mr Thomas: Lord Morris, I have already mentioned my general welcome to the speech. There was a specific paragraph there which I learnt about the previous evening, that I was going to be asked to carry out this review of information sharing alongside Dr Mark Walport, who is the Chief Executive of the Wellcome Trust, and I very much welcome the invitation. This is to be a fairly quick review—we have been asked to report by the middle of next year—a report into information sharing, which I think will look at both the public and private sector. Mark Walport and I only had our first meeting last week. We will have a small, independent secretariat to support us. The two of us have decided that we will be issuing a consultation paper at the earliest opportunity, to identify the main issues and to seek a wide range of views as to the best ways forward. I think that the review will provide a fresh opportunity to look at some difficult information sharing issues and try to draw a line under a debate that has been going on now for some four or five years in a rather unfocused way and giving a clear framework for the future. We have no preconceptions as to how the review will be undertaken but I think we are both agreed that information sharing as such is no panacea. Sometimes people think that just because you can share information you should do so and we are quite clear that that is not the right starting position; there should not be sharing of information just for its own sake. We equally recognise the values of information sharing for law enforcement, for improving public service transformation and so on. So what we will be doing is trying to identify where the boundary lines should be drawn as to what is acceptable and what is not acceptable and what safeguards should be put in place. Mark Walport was associated with a very welcome report published last year, which did not get very much attention. It was published by the Council for Science and Technology and that itself said, if I can summarise, that technology now allows so much information to be shared that we need to have much more awareness of this, and it said that just because you can share information you should not do so automatically. A very strong warning about the dangers of jeopardising public trust and confidence, and there was a very clear message there in the Council for Science Technology report that if you

jeopardise public trust and confidence you may undermine the very purposes you are seeking to achieve. A very similar message came out in the Royal Academy of Engineering report. I think it is quite interesting that we have two sets of experts, if you like, the technologists, both saying that technology can do almost anything these days and the cost of processing has come down, the cost of storage has come down but just because you can do it, be careful.

Q17 ***Lord Morris of Aberavon:*** I suppose it is too early to ask how the consensus that you referred to might be reached?
Mr Thomas: I think it is, Lord Morris; we are just starting this review.

Q18 ***Lord Morris of Aberavon:*** The collecting of private sector data by government, what dangers do you see from that? Are they going to be different from the public sector?
Mr Thomas: I think we are all aware how much information the private sector collects on us now. Our research shows that people value the confidentiality of their financial information at a very high level and the bankers' duty of confidentiality has always been an important area. Credit reference agencies collect vast amounts of information; airlines and travel companies collect information; we have mentioned supermarkets; Google, the history of our searches; Facebook and other social networking developments. The amount of information about each of us now being shared and passed domestically and internationally is quite staggering, and it is not surprising that the police and the security services, other public agencies can see some benefit in some cases for having greater access to that. But we are very clear that there are substantial dangers in any sort of free for all. It is a fundamental principle of data protection that information collected for one purpose should not be used for another unless certain requirements are met. So we are not saying that there should never be access to private sector databases, but we are saying that it should be controlled. I have mentioned the Serious Crime Act, which is concerned with the fight against fraud and we think that the balance there is the right one. There has been a lot of controversy about the United States' Department of Justice accessing the international monetary transfer system, SWIFT, and that was done without any public knowledge and it came to light last year and with our European colleagues we challenged the way in which SWIFT was processing billions of dollars and pounds of transfers every day and that information was being made available within the United States to security services there. Changes have now been made; they have been announced publicly by SWIFT and by our colleagues in the data protection community to put a tighter framework around that sort of access to information. I do not think your question can be answered in black and white terms. If there are legitimate, well defined purposes for accessing information, perhaps with proper authorisation from judges or in other ways to authorise it, that might be acceptable, but a free for all is not acceptable.

Q19 ***Lord Morris of Aberavon:*** What new powers do you seek?
Mr Thomas: Could I ask David to tell you a little bit about the proposals that we are putting forward to the Ministry of Justice about increasing our powers under the Data Protection Act?
Mr Smith: We have submitted a draft proposal to the Ministry of Justice. This is in two areas. One is to introduce a criminal offence for those who, broadly, knowingly and recklessly flout the data protection principles with a serious consequence. So say the doctor, the hospital that leaves the laptop in the back of the car with the patients' records on, it is hard to say that that is anything other than gross negligence. At the moment our power would only be to issue a notice to say that that should not happen again and if it happened again then there would be a criminal offence committed. That blatant breach of fundamental obligations should attract a criminal penalty. You can contrast it with the approach to security and the sort of information taken in the financial services sector, where the Financial Services Authority imposed the penalty and it was close on £1m on Nationwide, in similar circumstances—and I have to say not just because they had a laptop stolen but because that was illustrative of a lack of proper procedures. We are not seeking those sorts of powers but it is an anomaly that in financial services financial information, because of the risks to the market you can, as a business, face that sort of penalty, whereas if you fall outside those regulatory frameworks then all you fall back on is general data protection regulation where there is no penalty. The other area is a power to inspect. At the moment we can inspect the processing of personal data by organisations, public and private, but only with their consent—in only some very limited areas to do with European systems, Europol and so on, do we have a right to go in and say that we have come to make some checks. We are, as far as we can see, almost unique as a regulator in having a set of responsibilities to oversee and not then having a power to inspect that they are being put into practice. We think it will concentrate minds. We would concentrate any inspection power where the greatest risk applies, and we would not be able to inspect thousands and thousands of organisations, but it would help, we believe, to deliver data protection compliance and to get

business—public and private sector—to take data protection seriously.

Q20 ***Lord Lyell of Markyate:*** Very quickly, can we introduce a sense of proportion into this? I declare an interest, I have general practitioners in my family and they have to carry everybody's data about in their laptop. If they are going to be made criminals because they have made a mistake and leave it in the car you are out of proportion.
Mr Thomas: I do not think we would dispute that, Lord Lyell. The way we are putting forward the proposal is really quite narrowly focused and the example we have given is where a laptop with a lot of personal information is not sufficiently cared for and has not been encrypted. The technology now is available to encrypt a laptop and, frankly, any doctor and anyone else holding personal information should know the basics of making sure that the data is encrypted. Many examples of security breaches in recent years have brought home the imperative of that message. I am not seeking to criminalise a doctor for a single incident but when there has been gross negligence we need to have some sort of deterrent in place to make sure that people understand the importance of safeguarding the information. The proportionate approach is the one we are seeking to take.

Q21 ***Chairman:*** If I can move on to a different area, which you referred to implicitly a few minutes ago, which is the growth of these very unpleasant agencies who are parasitic upon the press in that they will obtain data nefariously or illegally which they then try to sell to newspapers as celebrity stories. I think I am right in saying that you reported in strong terms that people who indulge in this illegal collection of data should be subject to imprisonment and not merely a financial penalty, and I think that forms clause 75 of the Criminal Justice Bill at present in front of the Commons, and I wonder if you would like to give us your thinking both on this practice and also what the appropriate response to it is.
Mr Thomas: Section 55 of the Data Protection Act, which in effect has been there since the mid-1990s, is the only criminal measure in the Act at the moment, and that makes it a criminal offence to obtain personal information from a data controller, someone controlling a database, for example, without consent. Over the years we have investigated a number of these cases and we have brought prosecutions for some serious matters, which have resulted in derisory fines. We published the parliamentary report I mentioned earlier in May last year to document what we have been doing in this area, the nature and the extent of this quite pernicious black-market—a whole network of private investigators with a range of clients, including some financial institutions, some law firms, some local authorities even and representatives of the press are also the ultimate customers for this black-market. We obtained so much information about these activities that we were able to publish a tariff of how much it costs. For example, to find out who your family and friends are with British Telecom was costing between £60 and £80; a vehicle check at DVLA £70; a company director search £40; ex-directory phone numbers £40; mobile phone account enquiries £750. So there was almost a tariff which we were able to put together from the information we seized using our search warrant powers. We prosecute and at the back of the report we document the results we get. I have to say that I was a very angry Commissioner when one of the most serious cases resulted in conditional discharges for all concerned. I thought it was wholly inappropriate that the courts, with only a limited maximum penalty, were not able to impose far more serious penalties. So we published the report and we, amongst other things, called for the penalty to be increased to one of imprisonment—six months in the Magistrates' Court and two years on indictment in the Crown Court. We said that we do not want to lock people up but we do want a serious deterrent, and I am delighted that the government issued its own consultation paper following our report. Things have moved very fast indeed and as you said, quite rightly, Chairman, it is clause 75 of the Criminal Justice and Immigration Bill, which is currently before the Commons that does now contain provision to increase the penalties exactly in line with our proposal. It is not just that, we have also put forward proposals to the Law Society, the Financial Services Authority, the Office of Fair Trading, the Security Industry Authority, other bodies able to regulate this market far more tightly than has been the case so far.

Q22 ***Chairman:*** Have you included the Press Complaints Commission?
Mr Thomas: We have made recommendations to the Editors' Committee, which sits behind the Press Complaints Commission, but we have not been very enthused about their response so far. I spoke last week at the Society of Editors Conference and I had to say that, "I come here with my body armour on" because they had not been enthusiastic about this increase in penalties.

Q23 ***Chairman:*** These unpleasant vendors can only thrive if there is a market.
Mr Thomas: It is a supply and demand issue, Chairman. We have documented in our report some of the training manuals which we have found in some of these investigators' hands—they are the middle men, if you like. There are two main techniques they use. One is old fashioned payment—they find

somebody inside the organisation, whether it is inside a phone company or police station or other areas where vast amounts of information are collected, and they make payments to people, or they blag. Blagging is the term used in this context, which is to either impersonate the individual or to impersonate somebody else inside the organisation. And as you amass more and more information about the date of birth, the mother's maiden name, the address, postcode, you can build up a picture and then, using that, you can blag your way into an organisation. Another case is where they impersonate the organisation. The DWP in Humberside thought they were dealing with DWP in Belfast and for an hour and a half the person was on the telephone getting a lot of personal information before they worked out in Humberside that they were dealing with people who were not from the DWP inside Belfast. We have heard tape recordings of how they go about this business; it is a sophisticated business and we are very adamant that everything should be done to try and deter this sort of activity.

Q24 ***Chairman:*** Thank you very much. For those of us who have just only recently understood blogging, to get our minds around blagging as well is not easy!
Mr Thomas: It is "pretexting" in the United States; there have been a number of cases in the United States and in fact the Hewlett Packard Chief Executive had to resign because they were associated with this pretexting.

Q25 ***Lord Windlesham:*** You have really dealt with the question of the significance of the black-market. Do you think that the government should be doing more than it is and, if so, in what form?
Mr Thomas: Lord Windlesham, we are delighted that they have accepted our recommendation to increase the penalty, so full marks for doing that. I think also that the government is becoming increasingly aware of the risks. One of the first supporters of our proposal was the Department of Health. They are creating electronic health records. I think that something like 95,000 people within the health service will have access to those health records, and indeed the confidentiality and security around electronic health records is a major concern, and I very much welcome that. So they recognise that. First of all, they supported our call for increased penalties, but they also recognised the need for guidance and training and very clear messages to their staff about the risks of being duped by the blaggers and the consequences which would face anybody who improperly disclosed information, whether for payment or otherwise.
Lord Windlesham: I might just say that I am very impressed by what you have been saying. I think for those of us who do not have any special knowledge it is an eye opener to realise both the significance of the problem and the action that is being taken. It is not an invitation for complacency but it is the comment that occurs to me without knowledge, having listened to this short discussion on it.

Q26 ***Baroness O'Cathain:*** Regarding the future development of technologies, do you think that technology designers and providers are sufficiently aware of the privacy implications, when you see these geeks, these 17-year olds being able to hack into computers all over the world, not fully aware of the privacy implications. But longer term, the people who are developing the technologies which derive from the experiments of these young people, how are you going to ensure that they are aware of the privacy implications?
Mr Bamford: Perhaps I can help you on that one? We do recognise that technological developments can provide the infrastructure of the surveillance society in many ways, and indeed the combination of different technologies in a technological synergy can bring about to actual increases in surveillance. An obviously example is CCTV and then you have automatic number plate recognition technology, which is then allied with a database to retain all the information of the vehicles and the vehicle number plates, and then you use sophisticated data mining software to mine the information out of that, at the end of the day you end up with quite detailed pictures of people's travelling habits and things like that.

Q27 ***Baroness O'Cathain:*** And trackers as well.
Mr Bamford: That sort of thing. So we see how technology brings together certain risks and threats. It does not have to be like that on its own. We are very keen in the data protection community—and I think this is something which is gaining credence more widely—to deploy things which we call privacy enhancing technologies. The people who come up with all these technologies are clever people and they can think of more privacy friendly ways to actually process people's personal information, and we have seen that, as the Commissioner referred to with the Council for Science and Technology report. Also, the Royal Academy of Engineers did a report on a surveillance society and they used a phrase there about how engineers should exploit engineering ingenuity to protect personal privacy. It is an idea that we could actually use technology in a way which provides some sorts of safeguards. To use an example in Europe, in Austria they have an e-government programme there which involves government departments sharing information between each other, but they do it on a basis of certain computer algorithms, which means that the government departments cannot see all the data that is held by the

other department, they can only unlock what they need to in a particular transaction, and that is basically on the basis of an encryption key. That happens to be held by the Austrian Data Protection Commissioner in that country as a trusted third party to make sure it is used properly. There is an example of the big scale privacy enhancing approach. It can be done in a much smaller way—just putting encryption on a laptop is a way of providing some element of privacy protection there which is relatively simple and cost effective to do. We would hope that anybody who is developing technology and policy application should do it on the basis that they ask the people who are going to provide the technology to look at privacy friendly ways of using that technology. It is something which I think is striking a chime with the Department for Transport at the moment with its plans for road user charging, because they recognise that in theory you can build up a very, very detailed picture of vehicle movements as a result of a road user charging programme, and I do not need to explain to you the privacy risk that goes with that in terms of that big picture of how we all use our motor vehicles. They are looking at ways of doing this on a more privacy friendly basis, to actually restrict the amount of information that might be generated and what might be available in other ways. To use examples of information blagging that have been referred to before, clearly if you restrict the information in a system which is on view to people who do not need to see it then the privacy risk of blagging is less because less people have access to it.

Chairman: Thank you very much. We are going to run out of time, sadly, with our distinguished witnesses, so can I ask both your Lordships and the witnesses to be relatively brief so that we can cover as much ground as possible? Lord Woolf.

Q28 ***Lord Woolf:*** I am afraid my question is a little bit technical but perhaps you can answer it shortly? Part of your role is to create best practice. Do you agree that there are, so far as the legislation within which you work at the present time, unclear definitions that could do with clarifying? And if you do take that view perhaps you could indicate whether in this respect the Data Protection Act might well be amended to do it?

Mr Thomas: I think the Data Protection Act has had a rather poor reputation over the years. It is seen sometimes as being rather technocratic, rather obscure in some of its language. I said earlier, Lord Woolf, that the fundamental principles are actually written in plain English and I think are robust and I think serve us very well to this day, and I think we should not lose sight of those. The approach my office takes is to take a practical, down to earth commonsense approach to the interpretation of the legislation, and our strategic aim is to help the vast majority of organisations who want to get it right and to be tougher on the very small minority who are refusing to get it right. We want to help people; we now issue a very regular programme of guidance notes, and we try to make sure that none exceeds three pages or so—very short, targeted on the small businesses, and we find the large businesses find that quite helpful as well, and also public bodies. There are debates which happen in the courts, amongst lawyers and amongst the academic community about, shall we say, the definition of personal data. It is an important debate but perhaps only within those circles. It really only affects the very margins of our subject matter. On the changing definition—there has been a change because the European Commission felt that the UK interpretation as laid down by the Court of Appeal in the *Durant* case was not exactly the European Commission's understanding, and we have attempted to square that circle now; there is an Opinion from the so-called Article 29 Working Party and my own office has offered fresh guidance, if you like reconciling the Court of Appeal approach with the European approach. But in real life this only affects matters at the margins. The definition of personal data in the vast majority of cases has never been in dispute. We also hang a lot of weight upon reasonable expectations. I have tried to share with the Committee today how we have to respond to the societal context. If there are clear, legitimate purposes for collecting information that is a very important input to the way in which we interpret the law.

Q29 ***Lord Lyell of Markyate:*** Can I just start by saying that I very much support your approach and your work and your personal approach to it and I am sorry I had to jump in and ask for proportionality, but it is important and you said so. You want the power to do what you call a privacy impact assessment. Could you explain that to us?

Mr Thomas: I will start and my colleagues will do a far better job than I can. Essentially we are going to be publishing a handbook in about three weeks' time—we are holding a major conference in Manchester on surveillance society issues on December 11 and we have commissioned experts outside to help us develop a UK version of a privacy impact assessment. It is widely used in other parts of the world and it requires any major initiative, which is going to collect and use personal information, to go through a checklist as to showing how they have identified the risks, they have minimised the intrusion and they have put safeguards in place. So it is a checklist to ensure that some of the risks that we have been talking about this morning do not realise in practice. Jonathan is my expert on the subject.

Q30 ***Chairman:*** Could you make it the short version?
Mr Bamford: I will be a very brief expert on the subject, yes. Basically to deal with the original premise of your question, a privacy impact assessment would not be undertaken by the Commissioner's Office, it would be undertaken by the body who is developing the particular policy initiative because part of the process is deciding what to do so that they have a vision they need to get to and they use the privacy impact assessment—

Q31 ***Lord Lyell of Markyate:*** I am just going to cut you short, if I may. Tell me somebody on whom you might impose this because it might frighten a small businessman who suddenly gets a privacy impact assessment.
Mr Bamford: The vision in our mind is not of a small businessman; the vision is based on other jurisdictions where it tends to be public authorities who are actually engaging in the use of information that applies to lots of people, used for potentially sensitive purposes like health. Obvious examples that we have touched on this morning in terms of public policy initiatives would be ones like ID cards, would be ones like in England, Connecting for Health and the wider use of patients' information beyond their own surgeries. We would have issues to do with road user charging. Those would be ones where you would use the privacy impact assessment. We do not think this is a tool for use with a small businessman. We think this is dealt with at public policy level in many ways. Of course, a major corporation such as a major supermarket with a loyalty scheme may want to think about a privacy impact assessment with something like that, and a credit reference agency might; but the corner shop, we do not think it is right for that.

Q32 ***Lord Lyell of Markyate:*** I think it is important to say that you are safeguarding the public and you do not want to become part of the problem.
Mr Thomas: Absolutely not.
Chairman: We have two more questions: Lord Smith and Baroness Quin.

Q33 ***Lord Smith of Clifton:*** Do you think that the general public understand what happens to their personal data when it is collected by government or by companies whether online or in more conventional ways, and what evidence do we have of public concern about privacy?
Mr Thomas: By happy coincidence, Lord Smith, we are publishing today the results of our annual track. Every year we ask exactly the same questions of the general public through a mass survey and the results show, undoubtedly, that awareness is increasing and concerns are increasing. People care about the subject matter; we ask people to rank their social concerns and this year "Protecting my personal information" has ranked second out of all the possible concerns. It is second to preventing crime; it is ahead of concerns about the environment; it is ahead of concerns about unemployed; ahead of concerns about education; and ahead of concerns about health. So it has gone right up the agenda. We know now that something like nine out of ten people, 90 per cent, have concerns about the security of their personal information. The figure about whether you have lost control of the way in which your personal information is collected and processed is that now 60 per cent are saying that they feel they have lost control over the way in which their personal information is being used. Again, if I may suggest, Chairman, we will send the full research results, which are being published this morning—we are happy to share those with the Committee.
Chairman: We are very grateful, particularly the longitudinal comparison for the way attitudes are changing would be very helpful. Baroness Quin.

Q34 ***Baroness Quin:*** My two questions relate to coordination. The first is between yourselves and other Commissioners, the Interception of Communications Commissioner, the Surveillance Commissioner and the Intelligence Services Commissioner and so on. Do you have regular contact? Is there an overlap between the areas that you deal with and do you think that the coordination between you works?
Mr Thomas: Not very much contact on a regular basis because I think they have very discrete focused concerns which are not incompatible with our role—we co-exist perfectly well, we read their reports, we are aware of their activities and I am sure they read our reports—but we do not see a need for a regular programme of contact. But they have a very important role to play, the Surveillance Commissioner, the Interception of Communications Commissioner, the Intelligence Service Commissioner, but they are very specialised in their function—ours is a much, much broader remit. Your question also implied cooperation with our international colleagues because I think it is crucial to see these issues not just in domestic or UK terms. We all in the European Union work under the broad similar instruments at European level and we have very regular contact with our European colleagues, increasing contact now with our broad counterparts—it is not quite the same situation in the United States—but also Canada and Australia. A regular international Commissioners' conference every year—we hosted it in London last year—took place in Canada two months ago. There is a huge debate about these issues in the United States, The Patriot Act, and phone tapping issues in the United States, surveillance by the FBI, security breaches, so what happens there is mirrored across here and vice

versa—the debate is very lively over there as well as in this country. But I make no secret of my view that we need to have a far more global approach. I do not feel that we can have just a European approach; I think we have to find ways to reconcile the European approach with what is happening in the United States, in the Far East, South East Asia—all over the world, it is a global issue.

Q35 ***Baroness Quin:*** Are there any ways in which you have changed your own practice because of awareness of good practice elsewhere?
Mr Thomas: There are, yes, Baroness Quin. We published two months ago a data protection strategy setting out a more risk based approach to identify the detriments to individuals and to society, saying that we cannot do everything; we cannot adopt a conveyor belt approach, we are far more targeted now setting priorities, and we have developed that in conjunction with our colleagues elsewhere—they learn from us as we learn from them. The phrase we use is that we must all be "Selective to be effective". I am sorry it is a sound bite but it goes down well around the data protection community—we cannot do everything.
Chairman: We are not opposed to sound bites. Could I thank you and your colleagues very much, Mr Thomas, and say how impressed I think we all are by the work that the Commission is doing and how grateful we all are for the full and very helpful evidence that you have given us, and I hope we can come back to you during the course of our inquiry when we need to. Thank you very much.

Supplementary memorandum by the Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective.

2. During oral evidence given on 14 November 2007, the Commissioner offered to provide additional written evidence on the need for a greater obligation to be placed on the public sector to consult with the Commissioner when new initiatives are being proposed that present a significant risk to the privacy of citizens. The Commissioner is grateful for the opportunity to provide additional written evidence as the Committee continues its inquiry and update the Committee on developments since he last submitted evidence.

Consultation on New Policy

3. In his previous evidence, the Commissioner expressed his concerns that it is possible for policy developments in central government to proceed a long way before he is called upon to express a view, if he is at all. Although this is not always the case, consideration could be given to a more formal requirement on government and the wider public sector to seek the Commissioner's opinion on particular types of developments at an early stage.

4. To this end the Commissioner's staff have been investigating how central government departments consult with one another when a new initiative is proposed. While there is widespread consultation across central government, there is no formal process which the Commissioner can be included in. Much of the interdepartmental consultation relies on each department being proactive in consultation in any particular case.

5. Even where central government departments are willing to consult with the Commissioner's office, this is often only done at a quite a late stage in the development of policy. At this stage it is often difficult to take into account any privacy and data protection concerns that the Commissioner may raise. This can have the potential result of safeguards being implemented at a late stage as a compromise, and possibly more expensive, inadequate solution.

6. With the growing use of widespread collection, sharing, matching, mining and interrogation of personal information in both the public and private sector, a greater obligation to consult with the Commissioner at an early stage in the design and legislative process is essential. This would help to ensure that policies designed to protect individuals or deliver services more effectively are not undermined by data protection and privacy of concerns being neglected.

7. In addition, the failure to consult with the Commissioner can have a detrimental impact on Parliamentary time, such as when the Serious Crime Bill was submitted to Parliament and subsequent amendments had to be made during the passage of the legislation.

Consulting the Commissioner on Orders made under DPA

8. Section 67 of the Data Protection Act 1998 obliges the Secretary of State to consult the Commissioner before making an order or regulations under this Act[1], with only two incidental exceptions for fees and notification and the days upon which certain sections of the Act come into full force. It was the intention of Parliament that the Commissioner should be consulted on every order made under the Data Protection Act 1998.

9. While the Commissioner has been consulted on orders and regulations made under DPA, this has often not occurred until much later in the development of such orders. As such, the consultation has had less scope to affect the drafting of the resulting legislation or the policy thinking behind it.

Privacy Impact Assessments

10. In his previous evidence to the House of Lords Select Committee on the Constitution, the Commissioner had stated his intention to publish a privacy impact assessment handbook by the ICO by the end of 2007. The ICO PIA handbook was launched on 11 December 2007 at the ICO's *Surveillance society—turning debate into action* conference.

11. Over the coming year, the ICO intends to promote the use of the handbook as an important tool for ensuring privacy concerns are built into the design and implementation of significant new initiatives, developments and technologies in the public and private sectors. The ICO wants to work alongside those who decide to carry out a PIA, helping them with the process and learning from their experiences.

12. The Central Sponsor for Information Assurance at the Cabinet Office has contacted the ICO with a view to building PIAs into the guidance and direction they provide to central government in relation to information assurance. The ICO has also contacted the Office of Government Commerce in relation to the use of PIAs, as part of the Gateway Review process. This should help embed proper consideration of privacy concerns into the development of any significant new projects involving the use of personal information.

13. The Commissioner intends to learn the lessons of the first year of operation of the PIA handbook and conduct a review based on the experiences of those who have initiated a PIA at the end of 2008. The PIA handbook can be accessed at: http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html

Powers

14. In his previous written evidence and his oral evidence to the Committee, the Commissioner raised concerns about the limitations to his power to conduct an audit only with the consent of the data controller.

15. Since then, the Prime Minister has undertaken to provide the Commissioner with the authority to audit central government departments without their consent. The Commissioner has also provided a paper to the Ministry of Justice on powers he should be provided with to be able to regulate data protection more effectively and penalties which should be put in place for when the provisions of DPA are breached. This paper can be accessed at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf

16. The Ministry of Justice intends to initiate a wider consultation into the powers of the Commissioner over the coming months.

17. The Commissioner would ask the Committee to give consideration to the powers and penalties currently available under DPA, and whether or not these need to be increased to better regulate the collection and use of information about individuals within the UK.

[1] Section 67(3) of the Data Protection Act 1998 states:
Before making—
(a) an order under any provision of this Act other than section 75(3),
(b) any regulations under this Act other than notification regulations (as defined by section 16(2)),
the Secretary of State shall consult the Commissioner.

CCTV Code of Practice

18. During oral evidence provided to the Committee, the Commissioner mentioned that his office was in the process of revising the CCTV code of practice. This was published on 28 January 2008 at the ICO's celebration of European Data Protection Day at the Houses of Parliament. A copy of the CCTV Code of Practice is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

19. The revised CCTV code of practice clarifies the Commissioner's position on the use of cameras which can make audio recordings. The Commissioner would consider the use of cameras which record conversations to be highly intrusive and as such their use would only ever be justified in highly exceptional circumstances.

20. The CCTV code requires controllers of CCTV systems to assess the impact of the use of CCTV and to consider less privacy intrusive alternatives. This is particularly important as research has shown that CCTV may not always be the most effective measure for preventing or detecting crime[2]. With the use of CCTV becoming so widespread throughout the United Kingdom, it is important that those using the systems do so in a responsible and proportionate manner.

Conclusion

21. The Commissioner hopes that the information in this additional evidence is of assistance and hopes the Committee can give particular consideration to:

- creating a formal requirement for central government to consult with the Commissioner at an early stage in the development of new initiatives that present a significant risk to the privacy of citizens;
- recommend the use of PIAs to ensure that privacy concerns are properly addressed and these become a systematic consideration for all new significant projects involving the use of personal information; and
- improving the powers and penalties currently available under DPA, to better regulate surveillance and the collection of information about individuals within the UK.

Richard Thomas
Information Commissioner

11 March 2007

[2] See *"Crime prevention effects of closed circuit television: a systematic review"* by Brandon C Welsh and David P Farrington, Home Office Research Study 252, published by the Home Office in August 2002 and *"Assessing the impact of CCTV"* by Martin Gill and Angela Spriggs, Home Office Research Study 292, published by the Home Office in February 2005.

WEDNESDAY 28 NOVEMBER 2007

Present
Bledisloe, V
Goodlad, L (Chairman)
Lyell of Markyate, L
Morris of Aberavon, L
O'Cathain, B
Peston, L
Quin, B
Rodgers of Quarry Bank, L
Rowlands, L
Smith of Clifton, L
Woolf, L

Memorandum by the Surveillance Studies Network (Dr Kirstie Ball, Senior Lecturer in Organisation Studies at the Open University Business School, UK, Professor Stephen Graham, Professor of Human Geography, University of Durham, UK, Professor David Lyon, Professor of Sociology and Director of the Surveillance Project, Queens University, Canada, Dr David Murakami Wood, Lecturer in Town Planning, Newcastle University, UK, and Professor Clive Norris, Professor of Sociology and Deputy Director of the Centre for Criminological Research, University of Sheffield, UK)

The Surveillance Studies Network is a charitable company, registered with the UK Charities Commission, dedicated to public education on the subject of surveillance.

Executive Summary

The Surveillance Studies Network welcomes this inquiry by the House of Lords and the opportunity for further high level debate on the surveillance society that it offers. We make observations in five broad areas that we feel the committee should consider:

(i) Current Surveillance Practices, especially those which are of most concern;
(ii) Reasons for the increasing spread and intensification of surveillance;
(iii) Relationships between citizen and state; and,
(iv) Five models for society, including our favoured option of "The Reciprocal Society", which rebuilds trust and introduces assessment of the impact of surveillance technologies and processes.

We argue that the limitations of Data Protection and Freedom of Information law do not provide adequate protection for citizens in a world of pervasive (real-time, at-a-distance, computerised and automated) surveillance. Further that the nature of citizenship in such a society must be reconsidered and the constitution and law of Britain adjusted to reflect this.

Introduction

The Directors of the Surveillance Studies Network welcome the decision of the Committee to hold this inquiry. The details of our arguments may be found in our full revised Report *on the Surveillance Society*, which we append. We are making a submission separate from the Information Commissioner as there are significant differences of emphasis.

We outline four broad areas for consideration: current surveillance practices; reasons for the spread and intensification of surveillance; relationships between state and citizens; and, five models for society.

1. Current Surveillance Practices

1.1 Contemporary surveillance, often called the "new surveillance," or "digital surveillance", is characterised by:

— *pervasiveness*—surveillance tends to spread everywhere;
— *greater intensity*—surveillance is able to "dig deeper";
— *greater speed*—surveillance can happen quicker, even in "real time";

— *action at a distance*—surveillance can take place a long way from the person being surveilled;

— *interconnection*—different surveillance systems can be more easily linked, and information shared;

— *social sorting*—surveillance is aimed at categorising, sorting and profiling people based on "risk" or profitability;

— *automation*—surveillance is increasingly driven by computer systems and algorithms analyse collected data;

— *simulation and Pre-emption*—surveillance is tending towards anticipation of possible actions, risks and profits, and in many cases to simulate possibilities and pre-empt events;

— *data doubles*, the emergence of the virtual citizens composed of the information about us within databases, that stand for our real selves in all sort of transactions with the state.

1.2 The technological forms that characterise "new surveillance" are:

— *Computer databases*, which have added a distinctive dimension in that they are both searchable and remotely accessible. These databases are also increasing in scope, size and functionality.

— *Digital imaging and sensory technologies*, for example digital CCTV and scanning technologies, which allow storage of data, and algorithmic operations to be performed on that data.

— *Biometrics*, technologies that "recognise" individual or characteristic human bodily traits or movements, including facial recognition, iris scanning, movement recognition and so on.

— *Geolocation*, technologies that combine mapping and surveillance to track and control either individuals or patterns of behaviour, for example, satellite monitoring of offenders.

— *Micro- and Nano- technologies*, the decreasing size of sensors to the very small, including microcameras and "smart dust" or "motes".

— *Mobile technologies*, the increasing development of either temporarily-installed, remote-controlled or independently mobile systems, for example miniature Unmanned Aerial Vehicles (UAVs).

1.3 The characteristics and systems lead to increases both in targeted and mass surveillance.

— *By targeted surveillance* we refer to the surveillance of distinct individuals or groups, for a particular purpose.

— *By mass surveillance*, we refer to the undifferentiated and general surveillance of the population as a whole.

— Both of these take place, but the re-emergence of mass surveillance (which had been a key part of the authoritarian regimes of the mid-Twentieth Century) and the much greater use of intensive targeted and pre-emptive surveillance poses particular problems for constitutional rights in democracies like the UK.

2. Reasons for the Spread and Intensification of Surveillance

2.1 *Risk.* We live in a society obsessed by risk. Risk management techniques dealing with external threats have come a key part of organisational activities. Internal risk assessment procedures are also more common. The "war on terror" has made the "state of emergency" almost normal. We have seen the emergence of a "safety state" obsessed with security and stability, and increasingly favouring the precautionary surveillance of groups, categories and individuals by the state. This can confer personal and social benefits, but at the same time the conception of safety and security has important implications for liberty, privacy and other social values, as well as for innovation and change, which are inherently risky.

2.2 *Militarisation.* The obsession with risk is facilitating an increasing interchange between the military and civil realms. Technologies and assessment procedures that were pioneered in armed conflict are now seen on our streets, from "emergency powers" to stop and search, through Automatic Numberplate Recognition (ANPR) and the Geographic Positioning System (GPS) to Unmanned Aerial Vehicles (UAVs).

2.3 *Economics.* The security industry is one of the most profitable and fastest growing sectors of the global economy. R&D and promotion of new systems by the industry runs far ahead of the ability of bureaucrats and politicians to understand the systems, how they function separately and together, and particularly their longer-term implications for society and state-citizen relations. Sales pitches follow swiftly after key events like 9/11 or the Soham killings, and "silver bullets" are eagerly promulgated and too readily purchased.

2.4 *Information Society*. New generations are growing up information-literate and with new presumptions about their own visibility, privacy and exposure to surveillance. Those with greater access to knowledge resources are realising that it pays to try look after their "data double". This has become critical for life-chances, especially as credit scoring and other forms of database-driven rankings of the worthiness of individuals becomes the basis for the provision of a whole range of services.

3. Relationships between State and Citizens

3.1 There are multiple components to state-citizen relations, including:

- trust;
- justice;
- accountability;
- democracy;
- security;
- privacy;
- autonomy; and
- liberty.

3.2 The qualities of these relationships depend on the roles, power and performance of both state and citizens, and all are subject to both abuse and the development of dependencies.

3.3 *Trust*. There is clearly a decline of public trust in the state for many reasons. This is not aided by the use of exceptional/extreme arguments for every new security policy. The lesson of history suggests that states can and do fall prey to malign regimes, should we not be wary of creating an infrastructure that would greatly enhance their capacity to inflict harm.

3.4 *What is the right balance?* In the context of the deeper understanding of surveillance, talk of balance between "security" and "liberty" is highly misleading. We argue that liberty is an integral component of what makes security for citizens. Without liberty there is no citizenship, and there is only insecurity. Security is not a trump card.

3.5 *Where is the line crossed?* There is no one line to cross. Many lines have already been crossed: for example, we are watched by multiple CCTV systems in public places, and the police now have the right to take and retain intimate bodily samples even from those not charged with crimes. However a line crossed does not indicate irreversibility. There is no inevitable technological pathway predetermining how society and citizen-state relations should evolve. Genies can be put back in bottles.

3.6 *Is data simply information?* In the information society, citizens are made up of both physical and virtual characteristics. In terms of our relations with the state (and other institutions) we exist as much in databases as on the streets. Data therefore has a more intimate relationship with the physical person. In many ways we are data, and our "data doubles" are us. However the state sees the non-consensual acquisition of our data as its right, and citizens subject to punishment for withholding (eg: National Identity Register; proposed "stop and question" laws). This is archaic, and requires a rethinking of "data" in the constitution and in law.

3.7 *Can the state "opt out" of human rights?* There have been threats that the state might "opt out" of international human rights obligations, and roll back long-standing British legal rights. These rights are in most countries constitutional and irrevocable, the foundation of the relationship between state and citizen. Some might be new to Britain, but respect for these rights is what gives the state legitimacy. It is not for the state to decide to revoke them.

3.8 Crucially, the state should also be concerned about non-citizens. In a world of global flows, and porous borders, the position and treatment of non-citizens is crucial. Intensive and intrusive surveillance of non-citizens is not a sign of a mature society.

4. Five Models for Future Society

4.1 The Status Quo:

- We continue to rely on existing institutions and law, with the Data Protection Act (1998) and Freedom of Information Act (2001) and the Regulation of Investigatory Powers Act (2001), amongst others, as the bases.

— Codes of Practice and volunteerism predominate. The Information Commissioner is an effective but shackled regulator.

— The state is able to produce contingent arguments for exceptions and exemptions from human rights and existing constitutional protections and laws.

— Technological advances continue to run ahead of regulatory policy rather than designed with proper accountability and regulation built-in from the outset.

— The problem of trust is not addressed.

4.2 Laissez-Faire:

— The state encourages increasing privatisation and the development of a "Personal Information Economy", wherein personal data is a commodity.

— State and private sector pays market value of data it wants, but in turn citizen has to pay for access to information.

— Levels of "privacy" are set by these market relations and technological capacity. Citizens defend their privacy through Privacy-Enhancing Technologies (PETS), and you get the privacy you can afford within existing unequal market relations.

4.3 The Security State:

— The State of Emergency argument becomes the norm and security trumps all other considerations.

— Rights are permanently contingent on national security considerations. "Nothing to Hide, Nothing to Fear" is the motto.

— Citizen can obtain what information state feels is relevant and necessary, and the state can share data as it wishes and can change the purposes to which data is used as it wants.

4.4 The Transparent Society:

— The state prioritises information flow, and assumes that everything citizens do is public knowledge or liable to be known by the state and other citizens, but also that everything the state or private companies do is equally available.

— Minimal protections are created based on contracts between citizens and citizens and states, allowable in clearly-defined circumstances.

4.5 The Reciprocal Society:

— Create a new basis for information relationships between state and citizen with a comprehensive "Information Act".

— Liberty and privacy are considered to be an integral part of national security, not opposed to it, and surveillance and Freedom of Information are considered as reciprocal.

— Mandatory Surveillance Impact Assessment (SIA) for new technologies and systems, covering the social effects of the technologies and systems themselves and their interaction with other existing technologies and systems.

— Technologies are fitted to policies not vice-versa. Data-sharing is clearly about joined-up government, not "because we can."

— Citizens' data is treated as theirs—a kind of digital *habeus corpus*. States and companies are "custodians" of data not owners. Citizens have the rights to correct data, but custodians are responsible for errors and omissions.

— The ICO becomes a serious guardian of information rights and responsibilities, and of all surveillance relationships between state and citizen, and other institutions, with greater resources and strengthened oversight and audit capacities.

The only model we regard as both acceptable and workable is that of "The Reciprocal Society". If trust between state and citizen is to be rebuilt in a society built increasingly on information and surveillance, then a new constitutional settlement between state and citizens, and mature assessment of technologies and processes in the context of social purpose and effects are essential.

8 June 2007

Examination of Witnesses

Witnesses: PROFESSOR CLIVE NORRIS, Professor of Sociology, University of Sheffield, and DR DAVID MURAKAMI WOOD, Lecturer, School of Architecture Planning and Landscape, Newcastle University, examined.

Q36 ***Chairman:*** Professor Norris and Dr Murakami Wood, may I welcome you to the Committee and, in the case of Dr Murakami Wood, may I welcome you back to the Committee as I think that you participated in our seminar. May I ask you formally to identify yourselves for the oral record, please.
Dr Murakami Wood: My name is Dr David Murakami Wood; I am lecturer in town planning at the School of Architecture Planning and Landscape at the University of Newcastle upon Tyne and a researcher at the Global Urban Research Unit.
Professor Norris: I am Professor Clive Norris from the University of Sheffield. I am Head of Department of Sociological Studies and Deputy Director of the Centre for Criminological Research.

Q37 ***Chairman:*** Thank you very much indeed. You are very welcome and we are most grateful to you for coming. I said to the Committee that we have a large area to cover and I have asked that questions be brief and so, out of fairness, perhaps I could ask that replies should be fairly concise too. Gentlemen, your expertise is in the field of surveillance. Are you able to say how easy it is to define "surveillance" and to what extent it is possible, if at all, to break the concept into subcategories?
Dr Murakami Wood: There are a large number of definitions of surveillance, some of which would seem to cast almost all information gathering as surveillance and some of which would seem to only argue that "bad" forms of information gathering are surveillance. I think we would regard neither of these extremes as being useful definitions. We would argue that the intentionality is the important aspect. I think that information gathering with the intent to influence and control aspects of behaviour or activities of individuals or groups would be our working definition. So, it is the intention that we regard as important. However, we also argue that not all data that is gathered with no surveillance intention cannot become useful for surveillance in future and also there is the question of unintentional consequences of information gathering that are not thought of when the information is gathered.

Q38 ***Chairman:*** We are considering both surveillance and the use of personal data. To what extent can public sector use of databases of personal information be seen as a form of surveillance?
Dr Murakami Wood: In a brief sentence, we would say that it is possible to conceive of a database that is not used for some form of control. That is perfectly clear. However, it is equally impossible to conceive of one that could not be and I think that statement is about as far as we can really go with that.

Q39 ***Chairman:*** Are you able to say in what ways and to what extent surveillance by the state can contribute to public safety in general and be helpful to the individual?
Professor Norris: The state is responsible for providing security and clearly there is a whole range of people who may be considered a threat to that. So, databases of known individuals who are active in terrorism, drug dealing and so forth seem highly appropriate and I do not think anyone would want to argue that they are not. So, in the sense that the state has a duty to protect and to gather information of those it has good reason to consider to be a threat, then I think that one would say that this of course can lead to enhanced security and safety. I think it would be silly to think that surveillance is a "bad" thing or that the construction of databases in themselves is a "bad" thing. They have their uses and their places. For instance, the Sex Offenders' Register may be considered one of those things in general although, in its particular operation, one might have criticism of it. In that sense, there is not an argument that databases in themselves are problematic and they clearly can help in the administration of public safety.

Q40 ***Chairman:*** Are you able to tell us what information there is that CCTV has been as effective in deterring and detecting as was originally envisaged?
Professor Norris: "Little" I think is the short answer. When CCTV was first introduced in this country, it was not subject to systematic evaluation. It was introduced on the basis that practitioners thought that it was effective. Over the last ten years, studies have been carried out by academics and particularly the work by Jason Ditton in Glasgow and the work of Professor Martin Gill at the University of Leicester, which suggests overall that it has a very, very weak influence on reducing crime. The Gill study was published in 2004; it was the first major Home Office sponsored evaluation. Not only did it show that CCTV had very limited impact in reducing crime but it had very limited impact in reducing fear of crime. The evidence in terms of general reductions in crime and general reductions in fear of crime appears to be very, very weak. There are studies that do show a reduction in specific places. For instance, the same team that looked at Glasgow, the Ditton team, looked at Airdrie and, in Airdrie, they did find a reduction. In Glasgow, they found that crime increased when CCTV was introduced. One further study that is worth mentioning is the Farrington and Walsh meta-evaluation which also found very weak evidence for CCTV as a crime reduction measure; this again was sponsored by the Home Office. If I

remember correctly, they suggested at best about a three per cent reduction mainly in car parks and very little evidence that in town centre space you would see a reduction, but that street lighting seemed to be a rather more effective form of prevention.

Q41 ***Baroness O'Cathain:*** I have a very simple question particularly relating to your point about the fear of crime and showing that reductions in crime have not been affected by CCTV. Do you have any statistics at all about the reliability of these CCTV cameras? What proportion do you actually think are working? How many of them break down? Where do the manufacturers get a licence to produce them? Is there a special code or a specification for putting these up in the first place saying that they have to reach certain standards or can anybody string together some sort of camera and pretend that it is a CCTV camera?
Professor Norris: The answer to the first part of the question as to how reliable they are and whether there are statistics to tell us that, I do not know of any broad-range statistics on how reliable they are. Clearly, if you look at the Gill study of the implementation of range of systems, there were problems with reliability of systems and they were part of it, although I do not think they were necessarily wholly undermining of the systems but there were technological problems. The second part . . . ?

Q42 ***Baroness O'Cathain:*** Is there any organisation which actually looks at the manufacture of them, the actual physical specification?
Professor Norris: Certainly the Home Office has tried to issue guidelines.

Q43 ***Baroness O'Cathain:*** Tried to?
Professor Norris: Yes. I cannot answer your question with any certainty other than to say that they do issue guidelines as to what would be necessary in the technical sense. I think that the problem is that the range of possibilities is actually rather great, so specifying very exactly in any particular case what you can put in place and where is not such an easy job. One of the problems that has beset in a sense partly the expansion of systems is the problem of inter-operationability: different systems even in the same town and even run by the same council have different technical requirements, they do not integrate properly, and this still besets the industry.

Q44 ***Chairman:*** Do we understand from your answer to the first point of Lady O'Cathain's question that the reports we get in the newspapers of the number of cameras and the number of times we are all photographed are guesses and not based on any statistical evidence?
Professor Norris: I have to put my hands up to this because I am the originator of both these numbers. The number of 300 times a day that we are captured on film was included in a book I wrote called *The Maximum Surveillance Society*. Is it a guess, just a guess? I would say that it is a guesstimate. How I came to that figure was that I took a person in London moving around the City from early in the morning until late in the evening and I constructed a journey that intersected with known CCTV systems. So, this was not a fantasy in that sense, this was a journey. I think that I wrote this in 1998, so nine years ago, and I think that the estimate of 300 cameras was perfectly justifiable on what I knew about each of the systems that they intersected with.

Q45 ***Lord Rowlands:*** I am a little surprised by your initial answer because, for example, I travelled in on the number 24 bus this morning and inside the bus was a noticing saying that there was a CCTV camera and that there had been 60 prosecutions for vandalism. If you had polled that bus this morning, I would have thought that the vast majority of us would have said that it was an acceptable form of surveillance.
Professor Norris: I was not saying that it was acceptable or unacceptable, it was a question of how many there are.

Q46 ***Lord Rowlands:*** Yes, but you also implied that it was of very little value.
Professor Norris: I am saying that the best scientific evidence that we have does not suggest that CCTV surveillance is very effective at reducing general levels of crime.

Q47 ***Lord Smith of Clifton:*** Was this journey a journey which a number of people make or was it in search of CCTV cameras? Was it a deep search as opposed to a journey from Richmond to the City which a stockbroker might make?
Professor Norris: It was a busy day in London and it was trying to make a point so, in that sense, it was a piece of rhetoric. However, let us take my journey yesterday from the University of Sheffield to my hotel in London. Every stage of that journey was captured on a CCTV system. My university system captured me; on the bus that I caught to go into Sheffield to get to the station; as soon as I arrived at the station; I was captured when I got off at St Pancras; I was captured when I walked through to King's Cross, I was on their system; I walked into Smith's and I was on their system; I got into a taxi in London and that had a CCTV camera; I got dropped off at my hotel and, as soon as I walked into the entrance of my hotel, I was captured on a CCTV camera.

Q48 ***Lord Smith of Clifton:*** That was roughly 20 times; it was not 300.
Professor Norris: How many cameras are there? If we talking about the number of cameras that could have seen me, in the Underground there are thousands of cameras; in the stations there are thousands.
Lord Peston: I would like to ask a technical question following on from Lord Rowlands. Surely on Lord Rowlands' number 24 bus coming down from Hampstead no doubt.
Lord Rowlands: Coming from Pimlico.

Q49 ***Lord Peston:*** No one at the time you are travelling is a vandal, so that really does not count as evidence. The real point is that the vandals will be getting on later and they are not affected by those cameras. They are drunk, hooligans or what-have-you. Therefore, it is quite compatible that none of you were misbehaving but that the cameras had no impact on those who had a high propensity to misbehave. We do not know that, but we have to do the research and what we are being told is that the research shows that those who have a propensity to vandalise buses are not affected by the cameras. That does not surprise me at all.
Dr Murakami Wood: It is important to stress that neither Professor Norris and myself would argue that cameras are ineffective at adding to the weight of evidence or being used in court. I do not think we are saying that. The question was about prevention and the claims that were made for cameras when they were first introduced to actually reduce or prevent crime and I think it is quite clear from the evidence that we have seen that there is not enough evidence to suggest that there is any statistically significant effect on the rates of crime or any kind of crime prevention and that is the important distinction. It is up to you to make the judgment on whether that is important or not.

Q50 ***Baroness Quin:*** What evidence is there for displacement? In other words, if you have cameras in one place, crime just moves elsewhere. I can certainly think of an area that I knew quite well where crime was reduced by a very effective if somewhat intrusive CCTV system but at the same time crime rates just down the road rather increased.
Professor Norris: There is evidence for both displacement and for the halo effect. Certainly from the study in Doncaster conducted by David Skint city centre crime did reduce but it spread to the outer lying townships and there was statistically significant evidence to that effect. There have also been arguments for which you will also find some statistical evidence that, if you put a system in a particular geographical area, it could have effects on the surrounding areas which do not have cameras. Overall, the main level of effect is actually not very much.

Q51 ***Lord Morris of Aberavon:*** Does it not give a perception of safety to people when there are CCTV cameras?
Professor Norris: If you look at the evidence from the Gill study which is the largest study conducted, a three/four-year study funded by the Home Office employing a large number of researchers, their conclusions were that it did not increase people's feelings of public safety.

Q52 ***Lord Morris of Aberavon:*** It is the perception of people that I am asking about.
Professor Norris: Your feeling of safety is a perception. It did not increase people's perception that they were safer. In a way, we can see that that has been recognised. The whole of the city centre warden movement to having in a sense a visible authoritative presence on the street that is not necessarily police is about responding to that public demand that what they want is people not machines and technology and it is people who make people feel secure rather than machines.
Dr Murakami Wood: I have carried out a great deal of work in Japan and it is a useful comparison in this case because Japan is a society traditionally regarded as having a high level of social trust and very low crime rates in comparison to western countries. What I found from talking to people there, especially women—and CCTV is only now being introduced in public spaces with government support—is that, when they saw cameras, they felt less safe and not more safe because that made them think that the area was dangerous, that there was something they should watch out for. Whereas no cameras made them feel their normal level of trust in other people. It really depends on the level of social trust which you have in a society and I think that cameras are probably a mark of the decline in social trust and indeed may increase further that decline in social trust as we rely more and more on technology to replace and compensate for the decline in trust that exists overall in society.

Q53 ***Chairman:*** I have one final question on this before I ask Lord Smith to come in. Are you able to say what the evidence is of the effect of CCTV on detection?
Professor Norris: The simple answer to that is, "No, I cannot, not with any certainty".

Q54 ***Lord Smith of Clifton:*** What do you see as the key adverse effects of state surveillance? Do they go beyond the deleterious effects on individual privacy?

Professor Norris: Yes. One needs to think about this mainly in terms of mass surveillance rather than individualised and targeted surveillance. There are four broad issues here. Firstly, there is the issue that mass surveillance promotes the view in a sense that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted, and I think that that is a general issue. A second problem is that once you are into a surveillance solution, it becomes in a sense expansionary to a huge degree. If you see that information is what you need to solve a problem but you do not quite know what that problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people, and that is in a sense partly the way that things have gone. If one thinks about the new criminal records system which will integrate the databases of all police forces including all the intelligence files on 11 million people, I think it is 65 million records that will be integrated, all information comes to bear and then there is the idea that we have to join this all up. So, the information held in health fields, education fields and welfare fields all becomes part of the resource to solving a particular problem. The expansionary nature of a surveillance system is a problem if it does not have checks and brakes to it. The next point relates to what we said earlier. I think that there is an undue faith in technological solutions to the problem of crime, security and order. The best evidence is that order, crime and security are best promoted at a local face-to-face negotiated level. The best way for police to solve crime is if the public give them information freely. It is if the public trust the police that there is that flow. That is about a reciprocal relationship. One of the problems one has with reliance on technological solutions is that we can create a distance between police and public. We can see a police that actually see themselves as standing outside the community and coming down in a sense from the mountain to impose order rather than a police that are an integral part of that community who have to negotiate, sometimes with discretion and toleration, with various communities and individuals but, in that process of trade-off, what one does is build up trust and consent and consent is at the heart. I feel that the faith in technological solutions may actually lead to, in a sense, a shift from one of the fundamental principles of British policing. That would be my third point. My fourth and perhaps actually in a way the most serious issue is that, as one creates a mass surveillance system, as this personal information becomes more and more available, what we are seeing is the idea of risk assessments becoming more and more prevalent in various aspects of certainly criminal justice management but also within education and so forth, and the risk assessment provides the basis for pre-emptive intervention. I think that this is a really serious issue. The issue of course is that we normally talk about intervening with people in the criminal justice sense on the basis of individualised reasonable suspicion. Indeed, the PACE Codes of Conduct actually say that you cannot stop and search someone merely on the basis of a category such as their race. You have to have a better reason than that. Where you collect information and you say that if an individual who in a sense shares the characteristics of other individuals who deviate in some way and therefore are seen as criminal or whatever, that gives us the right to intervene with them and their families with various social programmes, some of which may have punitive elements to them. This seems to change and challenge in some ways and I am not sure that I understand all the ways it does, but ideas of reasonable suspicion and the presumption of innocence, for instance. Something is going on here that I think represents a fundamental shift which our concepts have not quite caught up with. I think that is how I would see the main adverse effects, but again I am particularly thinking about the mass targeted.

Q55 ***Lord Smith of Clifton:*** I would like to press you on this and it seems to me that you began to allude to this. Are there some categories of individuals or social groups who are adversely affected more than others?

Dr Murakami Wood: First of all, the thing to say is that both ends of the social spectrum, the most wealthy and the worst off, are both subject to high levels of surveillance. There is a big difference. Those at the top end of society tend to get the protective and inclusive benefits of this. This is surveillance that is voluntarily entered into for protection and for social inclusion in volunteering for systems like the iris scanning at Amsterdam Airport to speed you through immigration. You get better security, gated communities and things like that. At the bottom end however, there is significant deleterious effects on people's lives and Clive will detail some of these.

Professor Norris: If you look at the studies done on the operation of CCTV—and I think this raises one question about all these systems—generally these systems have elements of discretion built into them. They are not just automatic systems following automated routines; they involve people making choices. CCTV operatives have to make choices about who to target and the evidence is that they are most likely to target young males particularly if they are from ethnic minority communities. In terms of the way that that has an impact, actually it is not so much in the public sphere of the town centre, it is more in evidence in the private sphere of the shopping mall with what sorts of people tend to get excluded

from those areas. It is not just that they get excluded for criminal infraction, they are getting excluded because youths in a shopping mall are hanging about and they are not shopping and they are asked to move on. If they suggest that they have a right to be there, they are told that they do not. It is private space, so maybe they do not have a right to be there. Then they are excluded. If they argue too much, they will be banned from the shopping centre and the cameras and the security officers will enforce that ban. So, there is a form of exclusion that can go on which tends to target particular social groups and not generally us, as it were. If I may take another example, we have introduced mandatory drug testing in prisons. One of the features of such systems which seem to me to make them at least have elements of fairness in them is that they are random and, when they are random, everyone has an equal chance of being subjected to them. Unfortunately, there is also a little bit that says if a prison officer thinks that you warrant drug testing, then you will get it. This introduces again a human discretionary element to it. What I do not know is the extent to which that may be based on discriminatory bases. We do not know the answer to that question. As soon as you do that, you have that potential. I think that the DNA Register is one where this is really very serious. The over-representation of black men in the DNA Register is a serious issue and cause for concern and part of that over-representation is because they are more likely to be arrested by the police and in some ways that over-representation in arrest statistics may represent an over-representation in certain forms of crime but, in other ways, what it represents, as we know that those people are more likely to be arrested without charge, more likely to be acquitted and so forth, is that there is evidence that this is not just on the basis of good evidence. So, we have a system that is disproportionately including someone on a register which will affect their life chances in ways in the future which is based on forms of differentiation and I have suggested perhaps at times forms of discrimination.

Q56 ***Lord Morris of Aberavon:*** Am I getting the wrong impression? Is it that neither of you are keen on any form of surveillance or is that wrong? In your written evidence, you refer to "the emergence of a 'safety state' obsessed with security and stability, and increasingly favouring the precautionary surveillance of groups, categories and individuals . . . " What are the main dangers of this kind of approach?

Dr Murakami Wood: First of all, I think that it is very important to stress that we would never say that surveillance itself is a bad thing. If you read our report which we wrote on the surveillance society for the Information Commissioner, we are quite clear that surveillance is often about the best intentions regarding care and indeed many of our functions in a welfare society would not be able to work without surveillance. Indeed, safety and security of the Realm are also assured by surveillance in many cases. We would like to make it quite clear in the record that we are not suggesting that all surveillance is wrong or that surveillance necessarily has negative effects and Clive will talk about what we mean when we talk about precautionary surveillance.

Professor Norris: Again, it seems to me that there is this problem of if one is gathering information pre-emptively on a citizenry on the basis that they might commit future crimes, one is widening and changing the nature of the contract. If you look at the document on transformational government, it is clear that what is envisaged is basically a merging of all the data held by government in various forms. Information sharing and taking down the silos are key elements of that report. One of the questions for me here is that we have a regulatory system that has been built up on the principle that you give information for a particular purpose, but you give information in a context and it is to be used in that context. We now have a situation where it appears that what is emerging—and it is emerging—is that the context is merely governance, that you give information at one point of the system. So, as a child you have information recorded about you—I am not sure that you freely give it but it is certainly recorded of you and from you—and that can then become available at another point in the system, a criminal justice context for instance. This seems to be a change in the nature of how we have traditionally thought about information and about the extent to which people have the right to control information about themselves and how it is used. I think that that represents a significant shift. Does that answer your question?

Q57 ***Lord Morris of Aberavon:*** Up to a point only. You mentioned DNA testing. Presumably you would take an adverse view of the collating of information. You mentioned classes of people who will get on that register. What about the balance of advantage which might occur when people who have committed an offence 20 years ago are apprehended on the basis of information that happened to be stored? Would you put the ID card in the same category? Would you put the collating of health information, a study about which a large number of doctors are refusing to take part in, in the same category? Are they all in the same bag, as it were?

Professor Norris: No. In a sense, I think that the issue of the DNA register raises some very interesting questions. If we are as a society prepared to accept—and we seem to have been—that the police may arrest somebody, not charge them, take them DNA and store it on a register, then I am slightly concerned

because actually I think that the issue becomes, if merely arrest is the criteria for being on the register, (1) it gives the police a perverse incentive to arrest people because I think there is advantage to the police for having the register, it has definitely to be shown to be—

Q58 ***Lord Morris of Aberavon:*** An advantage to all of us maybe.
Professor Norris: But then I think the question becomes, if it is so advantageous, we should all be on the register. That is something that one might have to consider.

Q59 ***Lord Morris of Aberavon:*** Why not?
Professor Norris: I am not saying "Why not?" I think that is the debate to be had.

Q60 ***Lord Morris of Aberavon:*** What would be your view?
Professor Norris: My personal view is, given the unfairness that I think currently exists in the system, I would be prepared to sacrifice my particular bit of privacy in this to ensure fairness, but I suspect that there are others, intellectuals and academics, who would strongly disagree with that position.

Q61 ***Lord Rowlands:*** I am trying to establish whether you can define relevant information. For example, in his evidence, the Information Commissioner spoke about the whole business regarding the crime record and what is collected in there is irrelevant to the actual question about whether you can or cannot work with children. Is there any way in which we could devise a system where we could say, "That bureau has the right to relevant information and we define relevant information in the following way"?
Professor Norris: I do not know is the answer. One can see that that would be a response to this problem. One of the matters which comes into this is that security and crime control often do seem to trump all other issues. So, one of the questions would be, what would be the exceptions to the rule that stopped this? Where would you draw the line?

Q62 ***Lord Rowlands:*** For example, would the fact that I had nine points on my licence be relevant to whether or not I could work with children?
Professor Norris: It is interesting that you say that because I am someone who has to sign this for potential social workers and that is indeed an argument that gets had. I do not want to say how we resolve individual cases but certainly there are arguments on the committee which deals with these matters about whether it should or should not. Some people view that it should and some people view that it should not. My point is that it is never very easy to draw the line. We may think that a driving offence is seen as not being relevant. A driving offence that maybe severely injured a child would show a recklessness or could show a recklessness.

Q63 ***Lord Rowlands:*** That would be a criminal offence.
Professor Norris: Okay but being caught for speeding could have that effect and although it did not have in that particular case, it would be evidence that it might have. So, I think that points on the licence could be argued in that way.

Q64 ***Baroness Quin:*** Debates certainly here in Parliament often are framed in terms of talking about the balance between security and liberty. It was interesting that, in your written evidence, the Surveillance Studies Network evidence, it suggests that talk of balance between security and liberty is highly misleading because liberty is an integral component of what makes security for citizens and that, without liberty, there is no citizenship and there is only insecurity. Can you expand a little further on that for us.
Dr Murakami Wood: We put this in this way quite deliberately because there is this tendency to assume that the balance exists. What we are trying to say here first of all is that there are not equal quantities of this stuff on either side that you could take from one part and put in another part. We exist in a society of a kind of tacit social contract where we expect to be free and to have those freedoms protected and the main reason for security is to protect our rights to go about our daily business unhindered. Where that protection starts to remove those freedoms themselves, I think that tacit contract is challenged and it is a tacit contract in this country because we have no fundamental constitutional protections in the sense that some other countries have a written constitution. So, it is particularly important in a country like Britain where a lot of the contact is tacit. If those things are challenged, we generate a sense of insecurity and that is very important. Those senses of insecurity are in fact in some ways all we are left with. This can, in an extreme form, mean that you lose any meaningful sense of citizenship because, if you have no belonging, all you are left with is a sense of security where the state is no longer guaranteeing those things which you regarded as being part of that tacit contract. What is left is a void. You have no sense of citizenship. This case, in an extreme case, lead to that complete absence of citizenship, and that is an extreme and we have not reached that point in Britain. The key questions here are first of all, what is security? What are you arguing is security? What we are arguing is security from the beginning is that sense of guarantees for our liberties. Also, it is important to say what is being secured and we are also arguing that it is vitally important to consider

what is being secured by security. If what is being secured is ultimately just the state and what the state does, then, as far as I am concerned, that link with liberty is entirely lost. It becomes almost meaningless to talk about security if you are just securing the securors, if you are just securing the state. I think that it is vitally important and the reason why we put it in this way is that we are talking about securing liberties, not about playing off security and liberty. I know that that might sound like semantics, but I think that it is quite important because otherwise you allow certain things to be lost and the point is that there are some things that are always off the scales and they should not be included in any balance. We should not be putting everything in the balance. For example, I think that torture is always off the scales. Our American friends may disagree or some of them may disagree. Certainly, for us, I think that torture is always off the scales. You do not weigh up that particular item in a scale of security and liberty. I think that there are several other things that we would—and many of us would probably have different views on this—say are off the scales. That is why I think it is important not to say that there is just this balance. There are things that are not to be balanced and not to be included.

Lord Peston: May I take us on to the enormous growth in surveillance in our society certainly over at the age group of most of the people in this room, we have gone from when we were young with no concept of surveillance at all. Those of us who lived in the war had identity cards; I have never forgiven my parents for losing mine but that is by the way, but that was about it and there was no such thing as surveillance. A lot of what we now have is economics driven. We did not have supermarkets and, if you get supermarkets, you get shoplifting and then you get surveillance and it is quite clear what the cause is. It is not a higher propensity for people to be criminals, it is the fact that you create an environment in which criminality, in this case shoplifting, becomes the sort of thing one does. To go back to your class point, all my life middle classes have never regarded taking things through Customs illegally as a crime; it was regarded as a game and you always took more than you should through Customs.

Baroness O'Cathain: I certainly did not.

Q65 ***Lord Peston:*** So, there is a real class point here as well as everything else. I did not! Quite the contrary. Not being middle class, I have always been terribly frightened of the police and that goes back to another one of your points. Is the rise of surveillance very much economics driven is one question, and the other one is, is it supply side driven, namely firms make the relevant kind of equipment and then naturally they want to sell it and, for all I know, although I actually favour ID cards but in a much more limited sense that the Government are going for, there may a great industry ID lobby that intends to make billions out of ID cards?

Professor Norris: I would argue with you in that I do not know that there has been, in the way you are thinking of, such a growth in surveillance. I think that there has been a change in surveillance. When I used to come to Westminster to school—I went to Westminster City School in the 1970s—I used to get on a train. When I got on to the station, there was a platform guard and, when I got on to a train, there was also an end guard on the train, and that was whenever the station was open. The last time when I went to that particular station at 8.00 in the evening, there seemed to be no-one there at all. There was a help point which told me that I could press a button and that someone would answer and that I was being watched by CCTV. We have changed the nature of surveillance: conciergeship, face-to-face knowledge about people has changed. You are right in the sense that we did not necessarily see it as surveillance then. I think it is only when we have lost it that we understand that this had a control function often never put into practice because it was not needed because it was there. I think that is one thing. If you want to ask why there has been such a growth in surveillance in this country, one reason is because there has been little to stop it. The point about the constitution is, if you take, say, Germany, in Germany within the constitution, there are words to the effect that people have the right to self-determination and self-autonomy. One of the things that means is that you can appeal to the constitution about the presence of a camera because a camera is seen as reducing your ability to act autonomously because—and this is the way the Germans would argue—knowing that someone is watching you in a public space influences your behaviour and you are less free. That does not mean that you cannot have cameras in Germany. What it means is that you have to make a special plea as to why the camera is justified in that circumstance. So, it creates a brake. In Britain, in terms of cameras at least, there was no brake to be applied. There was no privacy law. There was no law to prevent cameras being put up. There was nothing to stop it and we had no higher appeal: we could not appeal to a privacy law because it was not there; we could not appeal to a constitutional principle like the Germans or maybe even the Americans or other states could. I think that that is very important. I think that, at a more general level as well, in continental Europe, surveillance is viewed at the public level with rather more suspicion and as something that is potentially dangerous. The reason for that is the experience of in the German state of being taken over by a fascist regime and then, in European countries, by being invaded and understanding what actually surveillance could mean

for particular sections of the population, and this notion that a state does not always act in the interests of its people. When it is being invaded, the occupying state clearly has mal-intention. I think that there is a danger in Britain that we see and perhaps with good regard that our Government are generally benign and have been. On the continent, they know that their governments have not necessarily been so benign. I think that we do have to recognise that the future is an unknown quantity. We do not know what 50 years will bring. Therefore, we need to think about, if we are setting up systems, what will the consequences be if, in two or three generations, our rulers are not so benign?

Chairman: I repeat my appeal for reasonable brevity.

Q66 ***Lord Lyell of Markyate:*** I want to talk about regulation and the improvement of regulatory policy—we do not have much regulation at the moment—about Smartdust, which I remember you told us about, and about Google Earth. As I understand it, you could be sitting in your garden and you could be watched by everybody who had access to Google Earth. Exactly how accurate it is at the moment we do not know, but I think we can anticipate that it will become or could become extraordinarily accurate. Smartdust could be scattered around the dining room table and all our conversation could be listened to. To what extent do you think those things should be regulated?

Dr Murakami Wood: This is at the heart of the matter here and I think that it is absolutely essential that we develop some ways of regulating these kinds of technologies. I would like to say how Google Earth is at the moment. It usually relies on stored satellite images and therefore on the whole is not conceived as a live image in many countries. In America, I think that they can produce relatively swift images but certainly not in most of the world yet, but you are right that this is just a technical impediment which will be overcome. Things like Smartdust do present an entirely new challenge because we are not looking at traditional forms of surveillance that can be seen. We are talking about all kinds of new technologies that present new challenges. Here, what we need is for policy to be able to deal with things that they have not conceived of previously in the past and the problem at the moment—and it goes back to your question about where this is coming from—is that the other driver of surveillance in this country is indeed the political economics driver, the driver of industry. Industries are producing more and more highly advanced technologies. That seemed to come as a complete package; it seemed to be a solution to social problems in a nice, neat technological bundle which is very attractive to policy makers. Easy solutions are very attractive. The problem is that the policy makers themselves—and that includes all of us here, the academics who study them even in social terms and the bureaucrats involved—usually lag way behind the technological development in terms of their ability to understand even how the technology itself works as advertised let alone how it works inside, inside the black box. If I asked any of you to tell me how an algorithm works for facial recognition, probably even those of you who had technical backgrounds might struggle and I study these things and I struggle sometimes to understand how a few lines of code can create certain kinds of effects within a piece of software. We need some very new kinds of regulations and this requires detailed technical knowledge and it requires somebody, a regulator or a regulatory body, to be able to say that this is or is not acceptable, not just an advisory committee but somebody to say, "No, this is not acceptable and we should not employ this technology". I think that there is a danger of us at the moment, especially in Government faced with the dangers of terrorism of crime, to say, "This technology looks like the silver bullet, it looks like the one that will solve the problem" and not consider what the bad effects might be and almost never to say, "No, that is a step too far" or "We do not want that" when presented with something that seems to solve a problem.

Q67 ***Viscount Bledisloe:*** In your paragraph 4.2.5, you call for a new and comprehensive Information Act to create the basis for the information relationship between the state and the citizen. What would be the principal components of such an Act and can you give us examples of statutes in other countries which contain these components?

Dr Murakami Wood: We are asking here for two things. First of all, to bring together the piecemeal and existing legislation that we have had in this country for a very long time. The British way in many ways has always been to do things gradually and introduce things bit by bit and this works in a context where things change slowly. We are looking in a context now where technological change is extremely rapid. For example, the Data Protection Act is conceived on the basis of an understanding of the computer that derives from the 1970s. Even though it was introduced in the 1990s, its understanding of computing is based on a much earlier period of understanding of what computers could do. We need to move ahead of the game. We need to bring together these various pieces of legislation that already exist first of all and understand their relationship. For example, the fact that freedom of information should be working in a reciprocal way with things that deal with surveillance, they should not be entirely separate domains, they should be connected. The first thing to do is bring together those existing pieces of legislation, start to connect them, start to see where the holes are, to fill those

holes and then to go further and to actually start to think in terms of the future about what might occur and how we might legislate for things that are now being developed or will be developed. Most importantly of all, this is about setting a framework for how Government and citizens should exist in the information society. We still have not really done this. Japan started to do this in the 1980s; they started to consider these issues and never really went that far but Japan started to do that. We never did. In the absence of conventionally understood constitutions, I think that this stage is a good time to take stock and to establish these new kinds of fundamental relationships between citizens and Government in an information society. So, understanding the information rights of citizens and understanding what information means to people.

Professor Norris: The other thing here is that if we say that personal data primarily should belong to the person in whom it originated, then what is the relationship between that person and the state's holding of it and how can that person audit the information that the state holds on them? I think that this becomes absolutely critical when that information is obtained without somebody's consent, that is without their voluntary consent. For instance, the DNA register is not a voluntary consent piece; you are coerced into giving your DNA for that. Similarly, CCTV cameras that record your number plates—and we are moving to a position now where the police will hold 50 million records of vehicle movements per day—is non-consensual. We have not consented to this act. I think as a citizen that, if the state is holding my personal information, the state should have a responsibility for demonstrating to me that it is accurate, that it is fair and that they have collected this information. How one manages that is problematic but I think that it is implied. These are things that we think an Information Act would have to start to grapple with and have some fundamental principles involved. However, neither of us are legislators and we would not say that we know that answer.

Q68 ***Lord Rowlands:*** Following on that, if a bill came forward on any new Information Act, what would you say about the Information Commissioner's powers? You call him an effective but shackled regulator. How would you unshackle him or how might he be unshackled?

Dr Murakami Wood: What we meant by this first of all is that we regard the current Information Commissioner as being an extremely active and effective regulator who has gone in some ways way beyond what he needed to do and has indeed sparked this whole debate in the first place. He is shackled in the sense that his powers are limited and indeed the powers of his office are limited. We would first of all see a requirement for a huge increase in resources for the Information Commissioner's Office. We would see the Information Commissioner as being the primary regulator of any kind of new information and in fact not just to be provided with the powers of inspection and prosecution that he would need for the state but also for private companies. I think that this is absolutely vital; we are talking about these vast new conglomerates of information like Google, Tesco Clubcard and so on. These need to be subject to inspection as much as the state and the state certainly does. Also, there should be not just a reactive set of powers but we would also like to see an active responsibility for the Information Commissioner to be not just a statutory consultee as is suggested here, but to have the right of veto over new technological developments. What I mean by that is that in several countries—and I am thinking of Canada here in particular—Privacy Commissioners are able to specify where or if certain kinds of technologies or systems are implemented. If we are going to have the technological expertise to assess these new things, these need to be vested in an authority which is trusted and which has a statutory function and I think that the Information Commissioner's Office would indeed be the place to put these functions.

Q69 ***Lord Rowlands:*** It sounds like a large, new empire in some ways. Some of them would become a sort of look-alike from . . .

Dr Murakami Wood: We have, for example, the National Audit Office when it comes to financial issues like this which is indeed a very large organisation and it has large responsibilities. I would suggest that in fact information is as important as finances for government and for governance and the relationships between citizens and government in the future and therefore it should be taken as seriously, funded as well and regarded with the same degree of statutory authority.

Q70 ***Baroness O'Cathain:*** How worried do you think the general public is about surveillance? How satisfactory is the public knowledge of surveillance or do they actually want to know about it because most people now exchange all this information on Facebook and the Internet and bringing the National Audit Office into it when you . . . It is quite a different subject. You could not control something that is blowing around in the ether throughout the world.

Professor Norris: I think that we have a serious job in educating our children about the dangers of some of their practices. Because children are doing this does not mean that it does not bring dangers. I have a son who uses Facebook and so forth and it clearly worries me about the level of personal information that can be obtained. I do not think that just because

they do it that we should say that it is okay because I am not convinced that it is and I think that we have a duty in some senses to create structures to protect youth from such follies.

Q71 ***Baroness O'Cathain:*** Let me pursue that. What sort of structures could protect people, because of the very nature of Facebook and the Internet and all this area, and dating agencies on the Internet?
Professor Norris: I think a growing awareness of the danger of allowing your personal information to circulate freely. There are ways of dealing with this.

Q72 ***Baroness O'Cathain:*** How?
Professor Norris: For instance, the conversation that I had with my son last week was to suggest that he did not disclose his real date of birth, that he lied on his Facebook. You can do that.

Q73 ***Chairman:*** Dr Murakami Wood, would you like to come in for the final word.
Dr Murakami Wood: What is important to remember with these kinds of systems is that they have only been around for three or four years. We are talking about incredibly new phenomena and these people are being very naïve and it is not just children. There was the case recently of a senior police officer who was also giving away large amounts of personal information.
Professor Norris: He is the Head of the Security Service.
Dr Murakami Wood: He was giving away plenty of personal information on his social networking site. A number of people are very naïve about these kind of systems and we have to remember that this will not be the final condition, if there is such a thing, of these systems in the future and that we will learn and in fact we will have to learn very soon. If you combine this with the issues we have seen in the last couple of weeks of the loss of 25/26 million people's data by Revenue and Customs, our naivety about the amount of information and how it is used out there has to come to an end very soon and it will do. I think that we are seeing the emergence slowly of what we are calling personal information economies where people start to take more charge of their person information, to realise its value and to take steps to protect it. We are seeing the rise of people like information brokers who will look after your personal data for you and create a better profile for you and people using things like credit referencing agencies to start to manipulate positively their data image on the web. I think that we will see a growth of knowledge. This will not be the final state but it is a very dangerous time and I think this is why we need this new set of legislation and why we need to take some responsibility when acting at this dangerous time.
Chairman: Thank you very much. Professor Norris and Dr Murakami Wood, may I thank you both very much on behalf of the Committee for being with us and for your evidence.

Examination of Witness

Witness: Professor Graham Greenleaf, Professor of Law, University of New South Wales, Australia, examined.

Q74 ***Chairman:*** Professor Greenleaf, good morning and thank you very much indeed for being with us.
Professor Greenleaf: Thank you very much for the invitation to appear before the Committee.

Q75 ***Lord Morris of Aberavon:*** I would like some comparison of surveillance in different countries. You have experience in your native Australia and other countries as well. How does the degree and nature of surveillance in our country compare with that of other countries? Are we much more restrictive than others or does it vary?

Professor Greenleaf: It varies. I cannot purport to be an expert on the details of surveillance in this country; I have picked up what information I can for comparative purposes and I will try to make some comments in comparison with, say, Australia and with Hong Kong which are perhaps the two places with which I am most familiar. In relation to Australia, I have, with the assistance of my colleagues, anticipating that the Committee would like some information about this, prepared some background information about the nitty-gritty of surveillance practices in Australia. I would like to hand that to the Committee. I would like to comment in summary. Australia and the UK could both be put at the more advanced end on the spectrum of surveillance orientated societies, but there are a number of differences between the two and overall I would say that the United Kingdom is probably further down the track of more intensive surveillance than Australia or at least going in that direction. I would like to pick up a couple of different indicia. There seems to be much more CCTV surveillance in the UK than in Australia. Whether the estimates of 4.2 million cameras are correct or just in the right ball park I do not know, but the Australian figures in the documents I have suggest numbers more in the tens of thousands for the largest capital cities. So, at most, you are going to be looking at only a fraction of the UK numbers and they are mainly, from my knowledge, orientated to transport systems and large crowd locations with some private sector use in large

supermarkets and the like. In relation to the ID card system that has been proposed or is in the process of being implemented in the UK, from what I know of it, this vast aggregation of data with very wide and uncertain purposes in both the public sector and the private sector goes far beyond any other systems with which I am familiar and seems to almost constitute the surveillance society in itself. You may be aware that the Australian Government were proposing to introduce what they call an access card for health and welfare benefits of which I have been a critic for some time. That is now not going to happen due to the change of Government in Australia in November 2007. So, on these particular indicia, Australia is going to be in the future a far less intensive surveillance society than the UK. Other factors such as the children's database, the NHS patient database with its very wide accesses and the DNA database, from what I know of them, the cumulative effect of these is far, far greater in the UK than the equivalents that do exist to some extent in Australia. If I may turn to the private sector, I think the big difference is that there are very few barriers in the UK to data sharing between different sub-sectors of the private sector, say between the credit industry, the insurance industry and the direct marketing industry. In Australia, because of legislation introduced in the early 1990s, information in the credit reporting sector is in effect siloed off from the rest of the private sector and that has made an enormous difference to developments in Australia compared, say, to the UK or the USA. So, quite a different picture. On the other hand, there may at the present perhaps be less government data matching at the moment in the UK than in Australia but, from what I have seen of recent announcements and committees looking at this, it seems as though the UK is catching up fast. One of the areas where there is very intensive surveillance in Australia is anti-money laundering where vast amounts of data are being sucked in by our money laundering agency from all sorts of cash dealers and any organisations involved in finance in the private sector. I suspect that there is more of that in Australia than there is here. May I mention something about Hong Kong by way of comparison as well?

Q76 ***Chairman:*** Yes.
Professor Greenleaf: I was a Distinguished Visiting Professor at the University of Hong Kong for a couple of years and that is why I have some knowledge about Hong Kong. I think that it is an interesting comparison, it having been a UK colony only a decade ago and now part of the People's Republic of China. Although Hong Kong was one of the first countries to introduce a multi-functional chip based Smart ID card, in fact its non-immigration uses are at present quite minor. The main criticisms that I and others have levelled at it is the potential for function creep in the future that has been built in. However, at present, it is not anything remotely like the UK system that is being developed. Data matching is quite limited in Hong Kong and must be approved by the Privacy Commissioner. I think that there is relatively little CCTV surveillance except in a few select areas of downtown entertainment areas of Hong Kong island, and not a whole lot more other than that. Transport surveillance is quite limited compared to what is being used. The Oyster Card here I gather is quite extensively used for police surveillance now. The Octopus Card is an anonymous smart card in Hong Kong and has very limited possible uses for surveillance. Telecommunication surveillance is also relatively limited. They have a new Interception Commissioner but the numbers involved are not very large. You can do things like get anonymous SIM cards for mobile phones by cash payments. Anonymous mobile phones is quite surprising in a jurisdiction which is part of the People's Republic of China.

Q77 ***Lord Woolf:*** You have already covered some of the matters that I was going to ask you about particularly because you have made a comparison between this country and Australia and then Hong Kong and of course a comparison between Australia and Hong Kong very briefly in what you have said. Having done so, do you think that part of the problem here is that our regulation at the present time is very piecemeal?
Professor Greenleaf: Yes, I do think that is part of the problem and this is not a problem that is limited to the UK by any means. Over the last 30 years, we have had the development at an international level of information privacy principles but there has been very little systematic development in the rest of the package, if we can call it that, of privacy principles, plus principles governing surveillance as such. These would make distinctions between overt surveillance and covert surveillance and what are the rules for each and whether there are different rules for workplace surveillance compared to open places and the like. Also, there are really no systematic sets of rules for intrusions of various types. I think that that leads to a lack of real rules in those latter areas which contributes to the proliferation of things like CCTV. It also means that neither Information Commissioners nor the general public nor the Parliament are able to get an overall grasp of what is the overall surveillance picture in our society and how these things are knitting together. We talk about the boiling frog but we do not really have much idea at what temperature from one year to the next the frog has reached. Yes, there is piecemeal regulation.

Q78 ***Lord Woolf:*** What is the answer to that? What is the solution you would like to see? Is that in turn piecemeal or is it one overriding form of protection?
Professor Greenleaf: I do not know that there is necessarily one answer to that. I think that you could have a general piece of privacy legislation which contains sets of principles for these various areas and maybe you could have one commissioner administering that but, in this country, I understand that you have commissioners for surveillance and commissioners for telecommunications interception as well as the Information Privacy Commissioner, as I will call him. That may still be a sensible model but it would be good if they were all working to one principle based set of privacy principles, even though they may administer parts of them differently. Picking up on the Information Commissioner's evidence last week, one thing that he did not say was that it would be good to have an annual "state of surveillance" report, that simply set out the facts on an annual basis of where each different type of surveillance had reached over the last 12 months and how they were now interconnected. That would enable Parliament, Government and everyone else to reach better policy decisions.

Q79 ***Lord Woolf:*** I think that there is the problem that can arise from what we have connected. We have had a very recent example of the problems of Revenue and Customs, one might almost say fiasco, with regard to the loss of information. Do you think that there are any lessons to be learned from that?
Professor Greenleaf: Yes, I think that there are a number of very serious lessons, particularly because that is what the future is going to comprise, in my view, if things are not changed. This is not going to be a one-off event. Some of the lessons that need to be learned are first that I think there has to be a serious acceptance of only collecting personal data where it really is necessary for organisations to collect it and not collecting it on some rainy day principle that it might come in handy some time in the future. I think that taking minimum necessary collection seriously has to be the starting point. In Australia, one additional principle that we have that is not found in the Directive or elsewhere is called the anonymity principle which says that organisations must provide services to individuals on an anonymous basis where it is feasible and lawful to do so. Our Law Reform Commission is currently proposing that that be extended to include pseudonimity as well so as to provide an additional level of protection against unwarranted disclosure of information. One other essential starting point for this is to get the acceptance of privacy as a value correctly included in our privacy laws. For me, what this means is essentially that the onus of justification of intrusion in any way into a person's privacy has to be on those who are proposing to do it, whether it be government, private sector or whatever. Basically, I think that is what is at the bottom of the German Constitutional Court's "informational self-determination" decision. They were not making privacy any sort of absolute right but they were making it very clear in the German context that every intrusion into privacy had to be justified up front in terms of alternative social benefits. Once you get that sort of starting point, I think that you can be on the right track and I think that that is a constitutional principle and a good reason for this Committee to be looking at this issue. That really goes to the relationship between the individual and the state.

Q80 ***Lord Lyell of Markyate:*** That leads very well onto Article 8 of the European Convention on Human Rights which gives everybody the entitlement to respect to their private and family life and that seems to come pretty close to what you are saying and might be built on. Bearing in mind the very rapid change in technology and the ability of those involved in surveillance or data collection to be much more intrusive than they are today, how do you think that our regulators should respond? Do they have the necessary powers and resources?
Professor Greenleaf: No, I do not think that they have either here or in most other countries although, if you pick and choose from the best of what various other countries offer, you can usually anywhere come up with a good set of improvements. I have already mentioned that I think that the Information Commissioner should have a role in producing an annual report on surveillance. When he gave evidence to this Committee, he mentioned that it would be good if he could help increase the effectiveness of parliamentary scrutiny by having a better ability to warn Parliament without having to be invited even to answer questions and the like. I would suggest going further than that and to give the Information Commissioner a statutory obligation to warn Parliament of any significant privacy dangers that he perceives in legislation or regulation. So, draw the line at "significant" so that he does not have to report every minor thing. In that way, he avoids having to justify why he intervened on a particular issue if he has a statutory obligation to do so and he cannot really be seen to be playing any partisan games in coming in on particular issues if that is his obligation. I think that it would be useful to give him that obligation and then it would be his responsibility if he did not do it properly. In his evidence, the Commissioner said that he may not have shouted loud enough about the DNA database. There would

be some comeback against him for not shouting loud enough about the DNA database to Parliament. May I mention a couple of other possible things or do you want me to stop?

Q81 ***Chairman:*** Very briefly because we have a great deal of material to cover in the next ten minutes.
Professor Greenleaf: Then perhaps it is more sensible for us to go on with further questions.

Q82 ***Viscount Bledisloe:*** You have very largely answered my question already when you were answering the questions of Lord Woolf. Am I right in understanding from you that you think there should be a comprehensive single statute on the right to privacy and that the onus should be on the person wishing to use your information or collect your information to justify that within defined grounds?
Professor Greenleaf: Yes, that is right, that is what I think. You could do that by not having just one statute but by having, say, a surveillance practices statute which effectively locked in with the information and privacy statute, but it might be more sensible to put it all in the one. I would like to say one further thing on that. On the question of privacy torts, I do not think that, in light of the case law in this country, there is any likelihood that a privacy tort will be developed by the courts. Although there are some developments in the area of breach of confidence that are useful, they will not cover other areas like surveillance. However, statutory tort provisions like those suggested by the Hong Kong Law Reform Commission in a very detailed report have been recommended by the Australian Law Reform Commission in its draft report and considered by the New South Wales Law Reform Commission. They could well just be included in an overall privacy statute.

Q83 ***Baroness O'Cathain:*** What are the limitations upon the exercise of individuals' consent to data collection and further processing and are they insuperable?
Professor Greenleaf: I think that consent is an instrument of limited value in privacy statutes and it has been somewhat abused by consent not being clearly enough defined. It easily becomes a question whether there is implied consent in circumstances where there is hardly any consent at all. Where genuine fully informed consent (where the individual really has the alternative to consent or not consent without being denied valuable services) is possible, of course it is one of the reasons that do justify what would otherwise be interferences with privacy. But where that fully genuine consent does not exist, it is better just to accept that the requirements should be first that there is justification for the interference and then notice that the interference is going to take place. I know that is a long way round to answer your question but what I am saying is that I think we should put consent in its proper place and not exaggerate its relevance to privacy laws.

Q84 ***Viscount Bledisloe:*** Are you really saying that every time one is required to fill in a form compulsorily, there should be a box at the bottom saying, "Do you consent to this being given to other departments" or "given to other people"?
Professor Greenleaf: No. What I am saying is that if you really do not have any choice but to consent, then let us not go through the charade of asking people to consent.

Q85 ***Viscount Bledisloe:*** Surely you always do. You have no choice but to fill in the form, but surely you should be given a choice as to whether it is then disseminated.
Professor Greenleaf: Yes, you should be given that choice unless there are very serious other social interests that mean that the information must be disseminated to others. Where those serious reasons exist and you are not going to get some social service or you are not going to get some private sector benefit unless you tick that box, then we should not be calling that consent.

Q86 ***Lord Rowlands:*** Is there sufficient international coordination in this whole field and is it possible or valuable to establish some kind of international standards of personal data practices and surveillance?
Professor Greenleaf: I do not think there is sufficient international coordination as yet. The shining example of good international coordination is the Article 29 Committee under the EU Directive where the Data Protection Commissioners of Europe have genuinely provided policy leadership for the whole of Europe. In the Asia Pacific region, our Privacy Commissioners, although they have a collective Asia Pacific Privacy Association, have not done that. They have not taken a policy development or a warning role at all, partly because there is no glue like the Directive to hold those countries' policies together. As a result, at a global level, commissioners are still rather hamstrung on reaching agreement about policy issues and have been very mild in their collective statements. To move on to the second part of your question, I think that there is still a very serious need to establish a standard for exports of personal data between countries. That is still a pressing issue and, as yet, the policy instruments that have been tried have not succeeded in delivering that. The adequacy decisions under the EU Directive which, if properly handled, might have forced an international standard on the world, if you like, have

not done that because the EU has lost credibility by caving into the USA and also because—

Q87 ***Lord Rowlands:*** How did they cave in?
Professor Greenleaf: They approved a proposal by the USA for its "safe harbour" proposals which, in most people's opinion, did not satisfy the adequacy tests under the EU Directive. However, for political reasons, the EU decided to let the USA go and the adequacy test lost a lot of its credibility as a result. They have also failed to reach decisions even about the most obvious jurisdictions to which they could have granted an adequacy finding like New Zealand or Hong Kong. The whole process, if it keeps going, will take to about the year 2099 before they get through most of the world.

Q88 ***Lord Rowlands:*** I am not sure that I understand what adequacy means.
Professor Greenleaf: For the purposes of EU countries under the Directive wishing to export personal data to countries outside the EU, it means that exports must be to a country that provides "adequate" data protection standards. But the EU Commission and the Council of Ministers make the decision—I should not go into EU Government matters—as to which countries meet that adequacy standard. So far they have only made a handful of decisions and the process is just bogged down and been discredited. The APEC Privacy Framework in my part of the world has contributed to undermining a search for a global standard. No UN conventions are really possible. The International Standards Organisation is not the right place to start for global policy. Surprisingly, I think that the only credible contender for the development of a global policy standard is to follow the direction or the lead of the Council of Europe Cybercrime Convention and consider using the Council of Europe Convention concerning data protection (Convention 108) as a way of bringing non-European countries into what could become a global standard. There are provisions in the Council of Europe Convention allowing this which have never been utilised. The Council of Europe can invite countries like, say, New Zealand to become a party to that convention. It is the only agreement I can see that could possibly turn into a global privacy standard which would not be too high a standard or too low a standard but somewhere in the middle.
Chairman: Professor Greenleaf, thank you very much indeed for being with us and thank you very much for your evidence.

WEDNESDAY 16 JANUARY 2008

Present
Bledisloe V
Goodlad L (Chairman)
Lyell of Markyate L
Morris of Aberavon L
Norton of Louth L
O'Cathain B
Peston L
Rodgers of Quarry Bank L
Rowlands L

Memorandum by the Association of Chief Police Officers (ACPO) Crime Business Area

PREPARED BY ASSISTANT CHIEF CONSTABLE NICK GARGAN

Summary

The Association of Chief Police Officers welcomes the decision of the House of Lords' Select Committee on the Constitution to conduct an Inquiry into the Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State. The Inquiry provides an opportunity to reflect on a range of issues which have been the subject of active scrutiny within ACPO in recent years.

The use of surveillance techniques, CCTV, Automated Number Plate Reader Technology and the acquisition of data from many sources are fundamental to effective law enforcement. Together they have saved many thousands of lives and prevented thousands of citizens from becoming victims of crime. The benefits are felt across society and help the law enforcement community manage threats which range from neighbourhood anti-social behaviour to international terrorism.

This submission will provide an initial, outline, response to the questions posed by the Committee's call for evidence and will go on to make more general observations on behalf of ACPO.

The Call for Evidence

In our response to the Committee's questions, ACPO sets out the view that:

- The reported descent into an Orwellian "Big Brother society" is more myth than reality.
- The development of widespread CCTV coverage is the result of a positive partnership between citizen and the State, rather than a degradation of the relationship between the two.
- Survey data indicates that citizens are very happy to support the development of surveillance and data acquisition mechanisms to achieve a balance between privacy and safety.
- The Regulation of Investigatory Powers Act 2000 (RIPA) has been an effective piece of legislation, but its implementation has placed an excessive bureaucratic burden on public authorities in relation to surveillance, in contrast to a much less regulated private sector.
- Technological advances have blurred the line between "surveillance" and "data collection". This is one of many reasons why it is now time to re-visit the Regulation of Investigatory Powers Act 2000.

Other Observations

The paper will go on to highlight the practical benefits and operational value of several techniques for data collection and surveillance.

The Association of Chief Police Officers

The Association of Chief Police Officers (ACPO) is an independent, professionally led, strategic body. In the public interest and, in equal and active partnership with Government and the Association of Police Authorities, ACPO leads and co-ordinates the direction and development of the police service in England, Wales and Northern Ireland. ACPO's 341 members are police officers of Assistant Chief Constable rank

(Commanders in the Metropolitan and City of London Police) and above and senior police staff managers in the 44 forces in England, Wales and Northern Ireland and other forces such as the British Transport Police and States of Jersey Police.

Specific Questions Raised by the Committee

Question 1: *How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and state in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

Response

It is not uncommon to hear media reports that we are "sleepwalking" into an Orwellian state. Research by Dr Benjamin Goold in 2004 explored the extent to which a surveillance society was developing: sustained by a "techno police". This new form of policing, linked to CCTV and other technological surveillance aids would become more authoritarian, better able to control public space and therefore increasingly less reliant on public cooperation. Goold's research with police forces in the south of England in 2004 suggested that this was more myth than reality. In fact, police policy and practice in town centres have not significantly changed as a result of widespread CCTV. The citizen sees that policing practice in respect of the law abiding remains largely unchanged, yet for the criminal the balance has changed (and not in his/her favour). The chances of being identified, arrested and convicted are much greater. In consequence of this, it is in many communities the citizen and the community itself that is driving the move towards greater CCTV coverage, often against the advice and better judgement of the "State".

Attached to the rear of this submission is a slide showing the results of a Citizen Panel survey. Conducted as a part of the *Review of RIPA 2004/2005*, this survey sought the views of the Leicestershire Citizens' Panel. Faced with a range of activities that might conceivably be carried out by the police, members of the Citizens' Panel were invited to indicate which should be done at officers' own discretion as a matter of routine, which should be done only with authorisation from supervisors of varying levels of seniority and which should not be done at all.

It should be noted that the most intrusive activity identified on the slide (breaking into suspects' homes) was considered to be completely unacceptable in all circumstances by fewer than 10% of respondents. More detail about this fascinating research can be made available, but the clear message is that the community is only too content to surrender some privacy in the interests of safety and crime reduction—and that CCTV is regarded as a highly acceptable intrusion.

Question 2: *What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might that line be identified?*

Response

There are few surveillance activities, or data collection techniques, that are of themselves good or bad. We would contend that the appropriate tests to apply when considering any techniques are the tests of legality, proportionality and necessity. The Human Rights Act provides an effective legal framework for applying these tests.

We support the principles set out by Lord Falconer, Justice Minister, in his recent campaign launch "Human Rights = Common Values, Common Sense". The sensible application of Human Rights to surveillance and data collection, analysis and retention should not be a driver for unnecessary bureaucracy.

Question 3: *What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

Response

The legislative framework to protect citizens' liberty and privacy is largely effective. The Data Protection Act 1998 provides good protection to the citizen and the Regulation of Investigatory Powers Act 2000 (and Police Act 1997) are effective in regulating the actions of public authorities. In 2004, a Review of RIPA was launched. The Review came about as a result of concerns that RIPA, although effective, was inefficient: a source of huge unnecessary bureaucracy. The Review found the legislation had several ambiguities and deficiencies and had been implemented poorly. There was diverse interpretation and application of the law, and the training provided within the law enforcement community had been piecemeal. Several sources of guidance had emerged—and sadly these would regularly contradict each other.

In particular, the Review identified a proliferation of unnecessary bureaucracy which was born of a generally "risk-averse" approach. This risk-aversion meant, and continues to mean to this day, that there is little in the way of domestic case law to guide investigators and Senior Investigating Officers. The prevailing safety first mindset offers little prospect of a challenge in the court room.

Whilst the use of surveillance techniques by the police and other public authorities is very tightly regulated, the same is not true of other users of surveillance. Advanced surveillance devices are readily accessible on the open market and proceedings for their misuse are very unusual.

Police colleagues are required to have a high level of authority before accumulating data that will provide a detailed picture of a person that will provide comprehensive information about their private lives—whereas other organisations, including large commercial organisations appear able to do so with impunity under RIPA, although the DPA 1998 applies.

The Committee may well conclude that this is an appropriate moment to recommend a rebalancing of the regulatory framework in circumstances that would reduce the burden of inappropriate bureaucracy on public authorities and put controls in place on other, currently less regulated, users of "surveillance". It would be, however, disadvantageous to introduce a regulatory regime that is costly and which discourages the use of private CCTV.

Question 4: *What impact do surveillance and data collection have on the character of citizenship in the 21st century, in terms of relations with the State?*

Response

As indicated above, in many contexts it is the citizen, not the State, who is driving this relationship. As RIPA progressed through parliament before 2000 there were widespread media reports about its very worrying implications. This public concern was quick to subside and the fact that policing practices have changed little as a consequence has reduced public concern. ACPO detects a widespread consensus that the use of surveillance and data collection have overwhelming public support.

Question 5: *To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?*

Response

In the view of the ACPO Data Protection and Freedom of Information Portfolio, the provisions of the 1998 Data Protection Act are fully sufficient to safeguard the constitutional rights with regard to the collection and use of surveillance or personal data. We should remember that the Act is based upon the European Directives and indeed our legislation has developed this even further in an effort to ensure that individual liberty is maintained.

Question 6: *Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

Response

ACPO acknowledges the need for independent scrutiny of the police use of covert techniques, and welcomes the likely benefit in terms of public confidence. The Office of Surveillance Commissioners supervises some of the police surveillance referred to above. But police forces are also subject of inspection by the Information Commissioner and the Interception of Communications Commissioner. These supervisory arrangements sit alongside the established inspectorate function for policing—Her Majesty's Inspectorate of Constabulary. We also identify the potential for overlap and duplication with the functions of the Commission for Equality and Human Rights.

The Commissioners' officers work entirely independently of each other and adopt different methodologies, have different styles and do not co-ordinate their inspection activities. ACPO favours a migration towards a single Inspectorate for the various activities covered within the scope of the Review. Current supervisory arrangements (Surveillance Commissioner, Information Commissioner, Interception of Communications Commissioner, etc) are inefficient, cause duplication and are anachronistic.

Two additional protections are suggested:

(a) A revision of the Regulation of Investigatory Powers Act to update the legislation in the light of developing technologies. This upgrading of the legislation would also enable greater clarity to be given in terms of the various definitions used in the Act.

(b) The Investigatory Powers Tribunal should be better marketed and understood, ensuring that citizens are more able to access and more likely to be aware of the protections that already are in place.

General Considerations Thought to be of Interest to the Committee:

CCTV

It is often suggested that there are 4.2 million surveillance cameras in the United Kingdom. This figure is an estimate, based on the number of cameras found on Putney High Street, London and then extrapolated to provide a figure for the United Kingdom as a whole. That was produced in 2002. The results of this study should be treated with caution. The same study found that 84% of surveillance cameras are operated by private businesses in shops, pubs, clubs and other commercial premises. The use of CCTV cameras in these "private places" is common practice in most western societies and in this respect, the United Kingdom differs little from many other countries in terms of the number or use of cameras involved.

The remaining 16% of surveillance cameras were identified as being located in those areas which can be described as "public space" and were operated by local authorities and other public agencies in places such as open streets, transport systems, hospitals and schools. It is the regular surveillance of public streets by local authority controlled cameras that sets the United Kingdom apart from many other countries in terms of CCTV surveillance. There is little use of street cameras in many European or North American countries, although this is beginning to change as governments begin to recognise the effectiveness of CCTV in the investigation of serious crime and terrorism. It is estimated that there are 30,000 street cameras in England and Wales, the majority operated by local authorities.

The availability of CCTV images greatly assists in the investigation of crime and disorder. Although the crime reduction capability of CCTV is sometimes disputed, the contribution to crime investigation is significant and the recovery of available CCTV evidence is one of the first actions taken during a major investigation. The contribution of CCTV images to crime investigation is not recorded in a systematic manner; it is likely to equal that of fingerprints and DNA in terms of its overall contribution to the detection of crime.

— ACPO identifies a number of recent terrorist investigations where CCTV images have played a substantial and significant part in two recent terrorist trials, each with national prominence, which simply would not have taken place had it not been for the availability of CCTV evidence.

— A case study from Merseyside Police reveals the use of ANPR and CCTV systems in connection with a specific operation, currently operated by Merseyside Police in the Liverpool and Wirral local authority areas. This operation, which is ongoing, uses the systems to locate and then track suspicious vehicles until dedicated police teams can stop them. To date, this policing activity alone has resulted in over 200 arrests and the seizure of 150 stolen vehicles.

— At a neighbourhood level, the following case is typical. In October 2006 a CCTV operator in Warrington became suspicious about the behaviour of youths walking through the town centre. For forty minutes the operator tracked the youths because he felt they were "looking for trouble". One of the youths suddenly armed himself with a large piece of wood and began a totally unprovoked attack on a young man in the street. The other youths quickly joined in. The CCTV operator used the police radio to summon help. Police arrived and two offenders were arrested near the scene. The third escaped but was later arrested after his CCTV image was published in the local press. The offenders were jailed for an offence of wounding with intent.

ACPO has produced a clear position paper highlighting the need for a strategy for the further development of CCTV in the United Kingdom. This strategy identifies the need for:

— Clear standards.
— Guidelines on registration, inspection and enforcement.
— Training.
— The police use of CCTV.
— Storage/volume/archiving/retention issues.
— Emerging technologies, changing threats, new and changing priorities.
— Partnership working.

The strategy has now been completed and is awaiting publication following Ministerial approval.

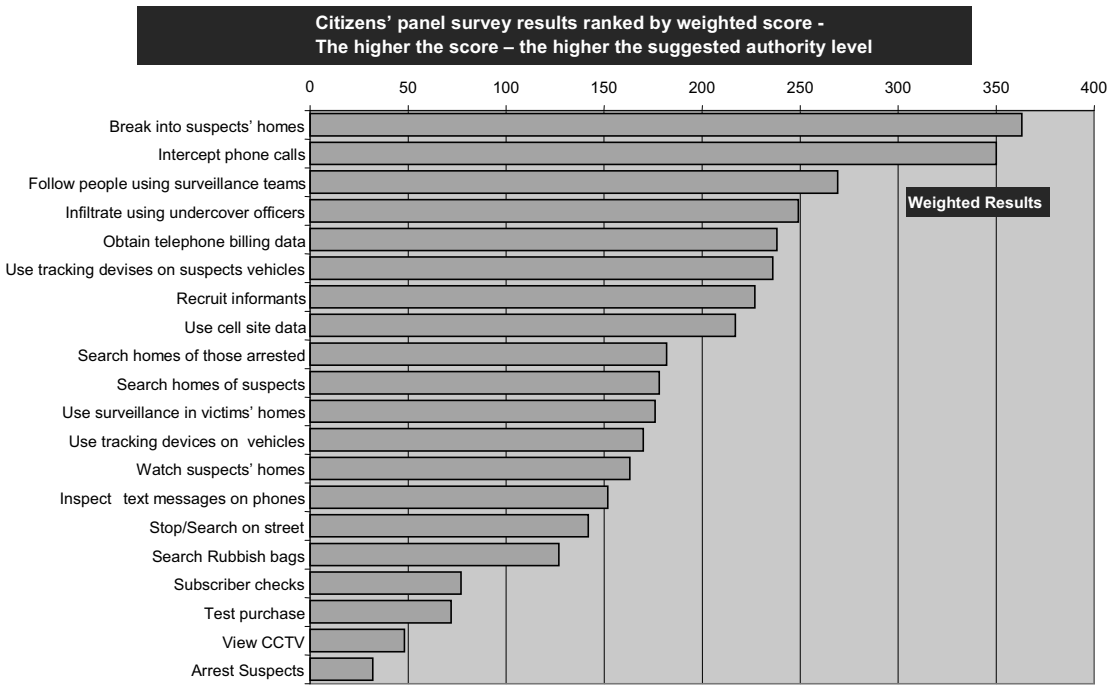
Directed and Intrusive Surveillance, Data Retrieval, ANPR and other techniques

The value of broader "surveillance" to policing extends far beyond CCTV. The acquisition, analysis and evidential use of data produced and stored in connection with everyday modern technologies is fundamental to crime investigation. The following examples from the Police Service of Northern Ireland are typical:

— The investigation into the Omagh bombing in which 29 people were murdered. Tracking the movements of mobile phones as they made or received calls using historic data was an essential part of this investigation.
— The conviction in Northern Ireland of Louis Maguire in April 2007 for murder relied heavily on evidence gathered by sensitive and intrusive techniques authorised under RIPA. Without this ability, there would have been insufficient evidence to convict Maguire and a dangerous criminal would still be at large.
— In March 2007, colleagues from the Police Service of Northern Ireland successfully traced the mobile telephone of a 17-year old girl who had left messages threatening suicide. She was discovered in a hotel bedroom having taken an overdose and was saved by police. Her life was only saved because public authorities were in a position to use data obtained under RIPA.

Without the ability to make lawful and effective use of these techniques, the effectiveness of the police service would be massively compromised.

APPENDIX



Memorandum by the National Policing Improvement Agency (NPIA)

Introduction

1. The National Policing Improvement Agency (NPIA) was established by the Police and Justice Act 2006 and is a Non Departmental Public Body (NDPB) which reports to the Home Secretary. The Agency is owned and governed through the tripartite NPIA Board which includes representatives of the Association of Chief Police Officers (ACPO), Association of Police Authorities (APA), the Metropolitan Police Service and the Home Office. This Memorandum sets out those areas of NPIA's work which we consider are likely to be of most interest to the Committee.

2. NPIA vested on 1 April 2007. It is sponsored and funded by the Home Office, but its executive leadership is drawn from the Police Service. The NPIA will support forces in improving the way they work across a range of policing activities and policy areas for policing in England and Wales. It will act as a central resource to ACPO and police forces, working closely with Police Authorities and the Home Office to help improve the way policing works. The NPIA's approach to improvement is centred on ensuring that people, process and technology change is managed coherently and forces provided with support and expertise to assist the implementation of national programmes of change.

3. NPIA's mission is to support the police service in reducing crime, maintaining order, bringing criminals to justice and protecting and reassuring the public by providing expertise in areas as diverse as information and communications technology, support to information and intelligence sharing, core police processes, managing change and recruiting, developing and deploying people.

Data Management and Data Sharing

4. In order to support the police service in reducing crime, maintaining order, bringing criminals to justice and protecting and reassuring the public, the NPIA will improve the way in which the service exploits information and intelligence so that it is used efficiently and effectively across policing and the wider criminal justice system. The NPIA will manage such data in accordance with relevant legislation (including the Data Protection Act 1998 and the Freedom of Information Act 2000) and established policies and guidelines on data management and data sharing (supporting the Transformational Government agenda).

Police National Computer (PNC)

5. NPIA's PNC Services is the service provider of the PNC, ViSOR (Violent or Sexual Offenders Register), NFLMS (National Firearms Licensing Management System) and shortly NABIS (National Ballistics Information System). ViSOR and NFLMS are accessed directly by forces/ enforcement agencies, and this will also apply to NABIS, but they are also linked directly to the PNC via an electronic interface.

6. The PNC came into existence in 1974 and has continually evolved since then. It comprises of four main databases:

- Names (the nominal details) of which there are over 8.6 million. With the introduction of NFLMS, this also now includes Firearms Certificate Holders. The PNC is used to make that information readily available and shared across all Police Forces.
- Drivers, 51 million.
- Vehicles, 57.5 million.
- Property, 96,000.

7. The use of PNC is controlled by three key documents:

- A statutory code of practice, The Police National Computer, effective from 1 January 2005.
- PNC Code of Connection.
- PNC Manual.

8. Access to PNC is available to all Police Forces of England, Wales and Scotland, together with the Police Service of Northern Ireland (PSNI). In addition it is accessed by a number of other authorised Agencies for specific purposes relating to law enforcement. Such access is controlled by ACPO's PNC Information Access Panel (PIAP).

9. The NPIA Board recently approved the creation of a new tripartite governance body, the Police National Database Operational Committee, to have overall responsibility for strategy and governance of Information Management in respect of the police national databases that are supported by NPIA's PNC Services. The terms of reference for the Committee provide clear accountability and responsibility for a single governing body to oversee these national databases. The Committee will have an Ethics group with independent members.

National DNA Database

10. The National DNA Database (NDNAD) is a key intelligence tool which has revolutionised the way the police can protect the public through identifying offenders and securing more convictions. The benefits of the NDNAD lie not only in detecting the guilty but in eliminating the innocent from inquiries, focusing the direction of inquiries resulting in savings in police time and in building public confidence that elusive offenders may be detected and brought to justice. Inclusion on the DNA Database does not signify a criminal record and there is no personal cost or material disadvantage to the individual simply by being on it.

11. The NDNAD Strategy Board provides governance and oversight of the operation of the NDNAD. Similar to the new Police National Database Operational Committee mentioned above (paragraph 9), it has tripartite governance involving ACPO, APA and the NPIA. The Strategy Board is chaired by the ACPO lead on forensic science.

12. The NPIA in conjunction with ACPO and the Home Office is responsible for policy on DNA and for assisting the police service in using it in the most effective and efficient way. The Agency also has responsibility for the delivery of National DNA Database (NDNAD) services and has a key role in maintaining and ensuring the integrity of the data entered and the use of the data in the investigation of crime. The NPIA understands there are improvements to be made in the management and delivery of the NDNAD and are working with the police to improve the processes. These include the reduction of duplicate entries on the database through the national roll-out of Livescan—a system of automatic fingerprinting terminals in every Police Force's custody unit. Another key development is the use of consent forms when taking samples from volunteers and witnesses for elimination purposes and the subsequent use of the data.

IMPACT: Information Sharing Between Police Forces

13. The IMPACT Programme, which is being led by NPIA, is helping to make communities safer by improving the ability of the Police Service to manage and share operational information to prevent and detect crime more efficiently. In doing so, it is delivering seven of the 31 Recommendations made by Sir Michael Bichard following his Independent Inquiry into the events surrounding the Soham murders.

14. The Programme is introducing new technologies, and helping the Service to implement the necessary business change, to exploit the benefits of improved quality and access to information across previously restrictive geographic and organisational boundaries.

15. The Programme has already delivered the IMPACT Nominal Index (which enables investigating officers in one force quickly to identify the existence of information relating to an individual (suspect) which may be held in a database by another police force in one of their key force databases). This has been rolled out to all UK forces and a number of key enforcement agencies. The Programme will ultimately deliver a Police National Database (PND); a single source of detailed information relating to people, objects (cars etc), locations and events that will link data currently held on local systems with that held on national systems such as the Police National Computer (PNC) and will address Recommendations 1 and 4 of the Bichard Inquiry.

16. The IMPACT Programme is also helping the Police Service to implement the requirements of the statutory Code of Practice on the Management of Police Information (MoPI) and the accompanying ACPO operational guidance.

17. The development of the PND does not create new operational databases and creates new information only in the sense that undiscovered links will be revealed and local force information will be visible to other authorised users of the system. The Programme is ensuring that the provisions of the Data Protection and Human Rights Acts, and other legislation, are observed and addressed; and that the impact on individual privacy is appropriate and minimised. NPIA is working closely with the Police Service, the Home Office, the Ministry of Justice and the Information Commissioner.

Automatic Number Plate Recognition (ANPR)

18. Since 2002, the Association of Chief Police Officers (ACPO) has promoted development of ANPR as a core policing tool, in conjunction with key partner agencies. ANPR is now overseen nationally by a multi-agency Programme Board, chaired by ACPO, with NPIA, HMIC, SOCA and the Security Service, amongst others, as members. ANPR has proven to be a very successful operational tool, enhancing the ability of the police to intercept, and arrest, a wide range of criminals using the roads.

19. In April 2007, the national work on ANPR was incorporated into NPIA which, under continued ACPO leadership, is responsible for operational ANPR services at a national level; a programme of Assisted Implementation in Forces beginning in autumn 2007; and co-ordination of the wider ANPR development programme.

December 2007

Examination of Witnesses

Witnesses: Chief Constable Peter Neyroud, Chief Executive of the National Policing Improvement Agency (NPIA); Assistant Chief Constable Nick Gargan, Chair, Covert Investigation (Legislation and Guidance) Peer Review Group, Association of Chief Police Officers (ACPO); and Deputy Chief Constable Graeme Gerrard, ACPO lead on CCTV, examined.

Q89 ***Chairman:*** Could I, on behalf of the Committee, express a very warm welcome to Chief Constable Neyroud, Assistant Chief Constable Gargan and Deputy Chief Constable Gerrard. We are not being televised but we are being broadcast. May I ask you to state your names for the record and then, if you would like to do so, make a short opening statement before the questions and answers begin.
Chief Constable Neyroud: I am Peter Neyroud. I am a Chief Constable but I am also the Chief Executive of the National Policing Improvement Agency.
Deputy Chief Constable Gerrard: I am Graeme Gerrard. I am Deputy Chief Constable of the Cheshire Constabulary and I chair the Association of Chief Police Officers' CCTV Working Group.
Assistant Chief Constable Gargan: My name is Nick Gargan. I am an Assistant Chief Constable with Thames Valley Police and until recently I have been Chair of the ACPO Peer Review Group looking at legislation and guidance in relation to covert investigation.

Q90 ***Chairman:*** Thank you. Would any or all of you like to make a short opening statement?

Chief Constable Neyroud: It might be particularly helpful in respect of the National Policing Improvement Agency because I guess for many of their Lordships this will be the first opportunity actually to have an engagement with NPIA. We are a relatively new organisation. It might be worth a couple of sentences on what our role is in respect of this area that we are dealing with today. NPIA was set up on 1 April. It is an NDPB of the Home Office but designed to be Police Service led and owned, and very obviously Police Service led and owned in terms of its Chief Executive. The areas that are particularly relevant in respect of today's discussion are: custodianship of major national operational databases and critical infrastructure, particularly the Police National Computer, the DNA database, the IDENT1 system and a range of other databases that support those; development and responsibility for developing programmes like the IMPACT programme and the Schengen Information System; doctrine— i.e. things like the Management of Police Information standard (we are responsible for developing that working to the Service's requirements); assisted implementation, which includes assisting the implementation of the Management of Police Information standards; and then research and evaluation. I think that gives the role and at least a start in terms of understanding where I may be coming from in terms of answering questions.

Deputy Chief Constable Gerrard: I do not have an opening statement.

Assistant Chief Constable Gargan: As the author of the submissions, may I highlight just one or two points that are made in there? The first point to make is that the use of covert surveillance is indispensable to the Police Service and to our colleagues involved in the fight against all forms of criminality. I would seek at regular intervals I would imagine this morning to emphasise the value of these techniques. In the submission, we have made the point on behalf of ACPO and on behalf of the Service that the often reported descent into some kind of Orwellian 'Big Brother' society is more myth than reality, that the development of a widespread CCTV coverage across England and Wales is the result of a positive partnership between the citizen and the state rather than as the result of a degradation in the relationship between the two. We have conducted surveys and the data from those surveys indicate that citizens are very happy to support the development of surveillance and of data acquisition mechanisms that achieve a balance between privacy and safety. We have looked in great detail at the Regulation of Investigatory Powers Act 2000 and found that this has been an effective piece of legislation. The implementation of that piece of legislation has been difficult and it has created an excessive burden of unnecessary bureaucracy, which is the source of regular complaint from operational colleagues and commanders up and down the country. We have worked very hard as ACPO and within the Service to do something about that excessive bureaucratic burden. Ultimately, our efforts have been partially successful in producing guidance for the Service. We are in the process of referring some of the things we have been unable to resolve back to the Police Minister in the hope that a fresh look at the legislation can now be taken. We think that is very timely, given the development of other technologies that blurred the line between data acquisition and conventional surveillance. We think that it is a fresh time to re-visit the legislation in its entirety.

Q91 ***Chairman:*** Could you please describe the main elements of the IMPACT programme for sharing data and the current state of its development?

Chief Constable Neyroud: There is a series of staged processes. The first one, which is already in active service, is the IMPACT Nominal Index. Basically, it is like the index in a large library that gives those that are accessing it access to the index level data from a whole range of operational systems that are held in local forces, enabling you to see data. For example, if you search for John Smith, you will find that there may be a record for John Smith in a number of different forces. What you cannot access is the record level data behind that; you have to go and seek that from a single point of contact in the individual force. Essentially, it allows you to go and find the data. It does not allow you actually to see it on the screen. That is supported by the Management of Police Information (MoPI) Code of Practice and the standards that fall beneath that which set out the ways in which information and intelligence that we are holding on those systems are reviewed and kept, and the way in which they are distributed as well. We have done two audits on that so far. The Service is making good progress towards achieving that standard, which is aimed to be at the point of full compliance in 2010 when the Police National Database goes live. The point to make is that it is extremely important that the MoPI standard is in place for when the Police National Database goes live in 2010/11. Then we have the PND, the Police National Database. Instead of simply linking the Index, you are linking the data behind that; it is the access to the record level data in a range of operational systems across forces. The final element of that is how we then link the PND to the existing operational data systems and in particular the PNC, which is a not uncomplex operation because they are two very different types of database. In essence, that is IMPACT.

Q92 ***Chairman:*** Can I ask what obstacles there are to the success of all this, whether cultural or organisational or data protection or human rights connected?
Chief Constable Neyroud: That is a bit of an essay question. First, you are right: there are cultural requirements because this is quite a significant shift. Firstly, you are not, as an investigator, simply going to be looking at the data held within your individual force. You are able to interrogate data, so your investigative parameters go wider and you need to think differently about how you use the data. There also goes with that the Management of Police Information standard, which is a much tougher standard on how you use the data and how we process and deal with the data and review it, et cetera. That also means that the data that you put in needs to be tightly controlled to that which is relevant and likely to be usable. In operational terms, the sheer quantity of data that the system will provide means that you need really to be focused about what you are asking and investigating. In human rights terms with MoPI, for example on Monday we launched the Equalities Diversity and Privacy Consultation around IMPACT. I believe we are the first organisation to launch a public consultation on privacy impact on a major national government system. I think I am right about that. I believe that if that is the case then the Police Service is leading the way. We are very serious about embedding those human rights and privacy implications into the running of the system.

Q93 ***Lord Peston:*** I was a little worried about the way you describe how this thing works in terms of possible waste of police resources. I take it what you do is input "John Smith", you said, and you get 20 hits, say. Now you have to ring up the 20 different police forces, is that right, and say, "My John Smith is a middle-aged, white man with a limp; is that possibly your one?" and he will then say "no", and you will do that 20 times. That is a hell of a lot of police time for what may be a very important investigation. Have you not thought that there might be some other route into this that saves a lot of time?
Chief Constable Neyroud: The first point is that at the moment, because at the moment we only have the access to the index level data, we have only deployed the system for public protection, and particularly child protection. We are only dealing with child protection units and researching that. We have restricted it. If we were doing that on the basis, for example, of investigating burglary across border, then I think your point would be well made but on public protection and given the way the system works, there are a number of different search fields on the system that would allow you to narrow it beyond that. It also works a little bit like Google on the basis of a probabilistic search, and so you are starting with a high level of probability that a match is there and therefore you are able to reduce the level of, as it were, speculative search quite quickly.

Q94 ***Chairman:*** In the light of the recent loss of data by the Revenue and Customs, are you confident that the Police National Database will be secure because presumably a very large number of people have access to it?
Chief Constable Neyroud: A very large number of people will have access to it but they will be people who are tightly controlled as working for the Police Service, having been vetted. Also, alongside the programme, which I did not mention in the introduction, we are also introducing a national system of identity and access management that will be tightly controlled in respect of the PND in particular, in much the same way as the PNC is currently tightly controlled as well in terms of individual access to the PNC. The way in which the database is constructed is that we are not drawing into the centre all of the individual databases into a single database in the centre. This database allows you, as it were, to top search the databases that are there and by creating a copy to be able to access it, rather than drawing all the data into the centre. It means that individual forces are actually controlling their data and continue to control their data, which I believe reduces the liability for very large quantities of data to be (a) moving around or (b) accessible in the way that has been suggested in other cases.

Q95 ***Lord Lyell of Markyate:*** Are there ways in which this might go seriously wrong? Could you give us an example of one of the nightmares you hope will not happen?
Chief Constable Neyroud: What are the nightmares I hope will not happen? There are not too many of them. Let us go down them. Creating a very substantial relational database is not without its complexities in technology terms. This is not an uncomplicated technology operation. The way I have de-risked that is by doing it in two phases. We are not going to envelope the Police National Computer; i.e. we are not going to imperil that key operational system whilst we are developing the PND. That is one nightmare that I hope we have mitigated. The second one I suppose is the issue that has already been touched on, which is those who should not be accessing the database, accessing it. We have put in the Identity and Access Management Programme in order to mitigate that risk. I suppose the third one is that it is such an important part of day-to-day policing that it will need to have substantial disaster recovery. We have had problems in the last 24

months with the PNC and a fire in Hemel Hempstead which took out a disaster recovery site on the PNC, so we are very familiar with the need for those major systems to have proper disaster recovery capability. That is inbuilt into the contract as we negotiate it. I would have thought those were the three. The other ones would be individual cases where the wrong information has been inputted into it. Given that the system will not result in a conviction—it is an intelligence database that will guide an investigation—I believe there are then further protections in terms of the Crown Prosecution Service and the court system that should mitigate those effects.

Q96 ***Lord Morris of Aberavon:*** Given, for example, the masses of knowledge which you refer to and couple that with the development of technology, and we are not dealing with a simple murder which has happened (preventable crime), does that not cry out for more time for investigation?
Chief Constable Neyroud: I am not sure I understand your question.

Q97 ***Lord Morris of Aberavon:*** In a simple case, which has happened, one can usually investigate within the normal parameters. Here you are in a new world with a mass of technology, hundreds of SIM cards and one possible conspirator. Is not the presence of the allowance that you have for time to complete the investigation made much more difficult by the mass of new knowledge and new sources and therefore you are up against it in doing it in time?
Chief Constable Neyroud: I think the short answer to that is yes. Having been a senior investigating officer in, as it were, the last era when we were just introducing DNA, it was tight in that era; it has certainly become tighter. It depends, and it depends whether you are dealing with a case where you have had to arrest the suspect early in the event, largely in those cases because of the public protection issues; i.e. not being able to let the suspect remain at large. In those circumstances, it is unquestionably the case that, even in the area of major crime, it is pretty tight to be able to get sufficient evidence together during the existing time limits. I think that is a fair point. Obviously there is a wider debate about counter-terrorism where the sheer quantities of information are immense and that same issue applies.

Q98 ***Baroness O'Cathain:*** This is just a very simple question. In view of the problems about hackers and security and your disaster recovery, I take it your information is encrypted?
Chief Constable Neyroud: It has a whole variety of different means of preventing that precise process happening.

Q99 ***Baroness O'Cathain:*** You did not actually answer the question. Is it or is it not encrypted? We all have firewalls; we all have virus checks; we all have all of that belt and braces stuff. The big issue of course with the later stuff from HM Revenue and Customs was that none of it was encrypted.
Chief Constable Neyroud: That was about data that actually left the data centre. That is a slightly different thing. We are not going to be moving and we do not move data out of our data centres on soft media unless it is actually handed from person to person. There are very few occasions when we do it from the PNC and we only do it on the basis of a person-to-person transaction with the person who is using it is doing so against signed instructions for the use and destruction of the material. In respect of the data in the Police National Database, what we have done is extremely careful work with the Government's CESG on the full information assurance of the system. I can only say, without going into the full details of that, that we have put a lot of effort into ensuring that this system is as secure as it can be. I appreciate that no database is completely secure because of course if you are giving people access into the system, your weak link is always going to be the people.

Q100 ***Baroness O'Cathain:*** Sure, but you think you are hacker-free?
Chief Constable Neyroud: We are doing our best to ensure that we are. No-one can promise that. The simplest element is, as it is with the PNC, the individual officer or member of staff who is acting corruptly. That is the simplest way, far simpler than seeking technologically to hack into the system.

Q101 ***Chairman:*** Could you say to what extent the data-sharing developments, which we have been discussing, in your view promote a preventative law enforcement strategy that is precautionary and intelligence-led, rather than one focused primarily on detecting the crime?
Chief Constable Neyroud: This was a very interesting question. One of the things I did in thinking and reflecting on this was to go back to the work that we had been doing on defining the business priorities in the system. It is just worth going through the five areas that we have in priority order: first, safeguarding children and vulnerable adults (that is fundamentally a preventive activity); second, counter-terrorism (and the bulk of the way in which we would use the data in that is preventive); third, proactive crime prevention and disruption; fourth, public, officer and staff safety; and it is only when we get to number five that we get into reactive criminal investigation. That is precisely the order of implementing the various elements of the PND. The

focus is very much on supporting the National Intelligence Model, which is the discipline that investigators operate to, and that is very much focused on identifying problems and applying a range of solutions to them in a tasked and focused way, which I believe is very much in the area of preventive approaches. The only qualification is this. The question implies that there is a dichotomy between prevention and detection. In certain crimes, for example in dealing with serious sexual assault, early arrest is an extremely important part of prevention as well. One of the pieces of work we have been doing is careful research on what will be the impact on Index for example and therefore potentially what will the PND actually deliver us in terms of added value in respect of major crime investigation. The early result of that—and we still have some work to make sure that these figures are hard and to develop the work further—is that in one in five rape cases there would have been additional information, that could have led to a detection. So that is a 20 per cent increase in the potential availability of information in serious sexual assault. One or two of your Lordships might point out that that is an area where we have a substantial amount of work to do to raise the bar in terms of effective investigation. I think it is a very important indication of the importance of this system for prevention and for public safety. After all, if you are looking at rights, the most important right, it seems to me, in terms of privacy is actually to be living free of crime because you cannot really have much privacy if you are not.

Q102 ***Chairman:*** Is there any evidence on the effectiveness of these technologies and databases?
Chief Constable Neyroud: There is a limited amount. There has been very little international research on the way in which the Police use technology. There have been really very few studies. That is one of the things the NPIA has been trying to do, to start doing some studies on the effectiveness of the databases as we roll them out, both in terms of what they can offer and also the best ways of using them, because there has been a shortfall in that territory.

Q103 ***Lord Rowlands:*** On international comparisons, are there equivalent systems elsewhere and how do ours compare?
Chief Constable Neyroud: This is a very interesting question because the other countries that we have regular contact with are moving very fast in similar directions. Obviously there are different national policing structures, different approaches between federal and local government, but in the last six to eight weeks I have been in discussion with the Australians, Canadians, Americans, Swedes and Dutch for example around the development of similar systems and the linkages between databases in those countries. There are very similar developments taking place. Canada, for example, is a country with a very strong record in human rights. We are working very closely together on developing the systems. They are supporting us with some ideas and we are supporting them.

Q104 ***Lord Rowlands:*** Are we ahead of the game or where do we stand?
Chief Constable Neyroud: In terms of the level of investment and the level of development in the last 10 years, I believe we are quite significantly ahead of most other countries.

Q105 ***Lord Norton of Louth:*** For any detail of the obvious benefits that may derive from the initiative, of course that has to be balanced against, for example, any potential threats to civil liberties, and this may touch on something you were saying a little earlier. What thought have you given to that dimension and to what extent do you think the existing safeguards are adequate? Do we need to enhance them—and it may come back to the comparative point—in drawing on experience elsewhere?
Chief Constable Neyroud: First, do we spend a lot of time thinking about this? Yes. We have not lightly gone out to do a public consultation on privacy, equality and diversity. There are two or three dimensions to human rights in these databases, one of which is who is on it and, secondly, does it disproportionately represent certain communities, for example. That is why it is extremely important to consult the public around that. The existing protections and the Data Protection Act and the Human Rights Act I think are a pretty good regime. In developing the database, we have taken a great deal of advice and worked very closely with the Office of the Information Commissioner. I would say that has been extremely helpful to us in shaping and dealing with some of the issues that would be regarded as issues in terms of proportionality and necessity. In terms of developing for the future, I think, as my colleague Nick Gargan said in the opening, that the bit to watch is whether the frame that we have is capable of coping with the way in which the technologies are overlapping. The Data Protection Act is more flexible but RIPA is one example in the legislation, which I think you are going to come on to, where it is very much the case that it has been designed on the fact that we have these pillared systems. One of the very obvious benefits, both to law enforcement and to public safety, is to stop the pillaring of systems and think about the connections. If I only took the issue of

responding to the parliamentary questions of your Lordships and others on the DNA database, it would be awfully nice if things joined up so that I could answer the questions. At the moment we have systems that have been devised in pillars. I think in many respects that is to the deficit of protecting human rights because it does not allow you to look across the whole piece. At the moment, my sense is that we have a pretty good framework.

Q106 ***Lord Norton of Louth:*** It will be a case of coming back to it, for the reason that you have just identified.
Chief Constable Neyroud: I think it is important that inquiries like this and other debates in public genuinely debate not just the ideas but actually look at exactly what it is that we are doing and the protections that we have. It seems to me that databases will work well and the public will have confidence if there is transparency and openness of the system, its operation and what they do, if there is integrity in the system and we can demonstrate that, and if there is a redress system under the Data Protection Act that allows the public to feel that if something is going wrong, they can put it right.

Q107 ***Lord Norton of Louth:*** I am not sure if you mentioned earlier on the consultation that you are undertaking what sort of timescale?
Chief Constable Neyroud: It runs till April. It is a full and public consultation.

Q108 ***Lord Morris of Aberavon:*** A major problem I have had is in assessing the balance in work I have recently done between the safety of the public and in sum total the state and individual liberty, whether they are vulnerable or not, embracing the whole of the public. How do you assess the balance and proportionality? Who is the best and most competent person to assess proportionality?
Chief Constable Neyroud: There are two or three things. Parliament sets the overall framework of operations. First of all, I operate within that framework. That is my starting point, the framework that I have been given. In a sense, it is extremely important that this type of inquiry and the one that the Home Affairs Select Committee is publishing explore whether Parliament's rules are sufficient to be able to describe the framework that is needed for that which we are doing. The second one is then that we look very carefully at the results that we are getting out of the systems. For example, with the DNA database, we look very carefully at the number of arrests that we are getting, the number of arrests it is contributing against the number of people on the database. We monitor very carefully the relationship between seeing samples and detections. I know that colleagues could tell you quite clearly within each of their forces what the level of success is in those terms, the types of crimes where it is being successful. I think it is important, particularly as we move towards a regime where Government is raising the bar on dealing with serious offences and particularly serious violent offences. In those cases, these databases are incredibly important in the investigation. Therefore, that is a key aspect of proportionality. It is not just about volume and quantity; it is also about seriousness.

Q109 ***Lord Morris of Aberavon:*** Obviously Parliament should be eternally vigilant and in particular keep up with all modern developments. Is the framework that you refer to sufficient for you to operate or should it be strengthened in any way?
Chief Constable Neyroud: I believe it is sufficient. Certainly, in running the databases, it is sufficient. It is supplemented by a range of published guidance like, for example, the Management of Police Information and the code, which is openly available, and then a range of guidance, some of which is confidential, for good reasons, which is again interpreting the overall framework. I believe that framework is pretty comprehensive and does provide some strong protections, plus you have the Information Commissioner and his ability to have a look at the systems. We are very open to the Information Commissioner coming in to look at our systems.

Q110 ***Viscount Bledisloe:*** I want to ask you about the retention of DNA information, bioinformation, beyond the period of the immediate investigation for which it was collected. Am I right in thinking that there are four categories of people for whom you may hold bioinformation: those who have been convicted; those who have been charged but not convicted; those who were arrested but never charged; and those who gave it voluntarily because they were on the scene or local enough to be useful. Are those the four categories of people whose data you will be holding?
Chief Constable Neyroud: There is one more, strictly speaking, which is law enforcement officials who may be on the scene: i.e. all of us have our DNA on the system as well, so there is one more.

Q111 ***Viscount Bledisloe:*** But you are all above suspicion.
Chief Constable Neyroud: May I say, my Lord, that if that were to be the case, that would be great.

Q112 ***Viscount Bledisloe:*** In your written evidence you say that inclusion on a database does not signify a criminal record and there is no personal cost or material disadvantage to an individual simply by

being on it. As a bare fact, I can see that, but that does not alter the fact, does it, that a lot of people who are on it would not want to be? You colleague is nodding.
Chief Constable Neyroud: I think that is fair. The DNA database only triggers if your DNA is found at a scene. It has no relationship to vetting and no relationship to other databases. Indeed, on access, the Police cannot access the DNA database; the only people who can access the DNA database are my custodian team and the FSS team that operates alongside that who do the work on putting data into the database and working on matches that have been requested. It is a tightly controlled system that is quite separate, for example, from CRB vetting. It is only there for the purposes of intelligence matches between individuals whose marks have come up for you to see. I think that is quite distinct from, for example, being within one of the intelligence groups or the PNC in those terms because there you are potentially triggering a CRB check, for example. I think that takes you into slightly different territory.

Q113 ***Viscount Bledisloe:*** I can see the logic in having the DNA of everybody who has been convicted. I can see a logic in having the DNA of the whole world or the whole population, but what is the possible justification in logic for the Police holding the DNA records of somebody who happened to be an innocent witness on the scene at a crime and not holding that of someone who was not there?
Chief Constable Neyroud: The innocent witness to a crime is asked to give his DNA voluntarily and can choose to have their DNA sample destroyed as part of that process or consent to the DNA profile being loaded on to the DNA database. There are some issues there around making sure people are properly informed at the time the sample is taken. There is a slightly different question. For example, Mr Huntley who was involved in the Soham case was arrested a considerable number of times before the events of Soham for offences that ranged between relatively minor potential sexual transgressions to quite significant ones. Mr Huntley would have, under the Criminal Justice Act 2003, appeared on the database. Prior to that he did not. That would have been a significant benefit to the investigation, and indeed the number of very serious cases that have been detected by the relatively small number of people in terms of the proportion of the database who are on there who had not subsequently been convicted is a very significant part of the overall package of investigation.

Q114 ***Viscount Bledisloe:*** I am asking about people who have never been suspected of any crime but because it happened in their house or in their community have given their data without much thought but without really realising it would still be there in 20 years' time.
Chief Constable Neyroud: That comes down to making sure that people are properly informed when they are asked to provide the sample what the implications are and what the process would be if they seek to have that sample taken back off the system.

Q115 ***Viscount Bledisloe:*** What is the process?
Chief Constable Neyroud: The general process is that they should be properly informed and they should be told that they can apply to have their data removed. In respect of volunteers, the process is that they can choose to have their DNA sample destroyed or consent to the profile being loaded on to the DNA database. There was a question provided to us in advance around the Ethics Committee. One of the issues that the Independent Ethics Committee is looking at is the issue of volunteers because it is an important component of the database. We are anxious to have high levels of public confidence in the mechanisms, particularly for volunteers in those circumstances.

Q116 ***Viscount Bledisloe:*** Do you at the very least not retain it unless they have positively consented rather than the other way round?
Chief Constable Neyroud: They should have positively consented in the sense they have been asked whether they would be prepared to give. It is difficult to take without consent.

Q117 ***Viscount Bledisloe:*** I am perfectly happy to give my DNA supposing my girlfriend is murdered in my house or something, but I am not particularly happy that it should remain there for the next 20 years after the person who murdered her has been convicted and the whole file is closed.
Chief Constable Neyroud: That is understandable.

Q118 ***Viscount Bledisloe:*** Should it be removed unless I have said, "Yes, you may keep it"?
Chief Constable Neyroud: That goes back to what the original informed consent is about, making sure that is tied down and people understand what the implications of that are.

Q119 ***Lord Peston:*** There are some of us who believe there should be a national DNA database and that this should never arise. I take it that the innocent people's DNA is taken so that if you find a suspect, you know that that is different from what you have taken. It may be 20 years until you find a suspect for an unsolved crime and suddenly to discover that you have given away the DNA of the innocent person makes your life more difficult. I am really not in agreement with Lord Bledisloe but I am clearly much

more of a reactionary than he is. I think we should have a national DNA database that you can just check everything off.

Chief Constable Neyroud: Yes, and I do not mean yes, I agree with that. I think I would be the poor soul who would be asked to implement it. I would comment on that. It is an interesting debate but that would be a very substantial investment and would pose a whole range of other issues. I do understand the point. Where the line is drawn—and incidentally that is not a matter for me, it is a matter for Parliament where that line is drawn—is, it seems to me, a very proper matter of debate. I think it is up to me to demonstrate what it is that we are doing with the DNA samples of those who are on the database. I do think that probably the most popular parliamentary question is around the various categories and what the results are. The level of results in terms of serious crime detection on those who are on the database who have not subsequently been charged or convicted is very considerable indeed.

Q120 ***Lord Lyell of Markyate:*** With the direction we are going, I think some members of the public (and that might include me) tend to think that the Police, for reasons which have some justification, would like the database to be as big as possible. The whole idea of not returning or not disposing of people's DNA unless they actually come and ask for it seems to be slightly curious. If you have somebody who you are satisfied is an innocent bystander or a volunteer, why is it not just cleared from the database straight away? It would make the database more manageable and it might be comforting to citizens.

Chief Constable Neyroud: I think the point made by Lord Peston is an extremely important component in that. Just to make the point, it is not our ambition to have the largest database. The Police Service is not in a competition about who has the largest database. It is a very important point. The Police Service's case to Government when the last changes to the database were made was about the strong likelihood of serious crime detections that were there as a result of expanding the envelope beyond those who were convicted of a recordable offence or cautioned. That has indeed proved to be the case. In terms of wishing to expand it by just sort of accidentally keeping a load of records, no, that is not our ambition. Our ambition is to have a database that secures wide public confidence and is an effective investigative tool.

Q121 ***Chairman:*** Chief Constable, before Lady O'Cathain comes in, can I ask if there is a difference between the practice in Scotland from that in England and Wales?

Chief Constable Neyroud: There is a separate DNA database in Scotland whose samples are submitted to the DNA Database in England and Wales. There are some small differences, and they relate to the rules for keeping the records of those who were not subsequently convicted. It is not a blanket process of retaining all of those who are arrested for a recordable offence. There is a step down in relation to those who are not subsequently convicted, for example, of a serious sexual assault. There is some provision for retaining those records, but not more widely.

Q122 ***Baroness O'Cathain:*** Chief Constable, you said it was not your ambition to have the largest database and I am sure it is not because there must be a lot of problems. You also said that the cost of having a national, totally statutory database that every one of us would have to be on would be very large indeed. Do you think that the national DNA Database Ethics Advisory Group would be looking at the option of having a national database with everyone on it versus an identity card and the cost there involved or can you tell me what else the National DNA Database Ethics Advisory Group is supposed to do?

Chief Constable Neyroud: I do not think initially they would be looking at those particular questions. The first set of things that they are looking at are many of the issues that have been raised here this morning around confidence that the balance between the proportionality or the necessity of holding data for arrest and detection has been properly balanced with a sense that the public would have confidence in that approach. That is very much their first look. They are looking at two particular sets of issues, one of which we have done as an agency: an equality and diversity impact assessment of the database. One of the other issues that was raised, in fact it has been raised in both Houses, is that of proportionality in terms of the ethnicity of those on the database. That is one issue that they have been looking at and we have been looking at very seriously. The second issue is around the rules and the redress issues on the database, which are, as a number of their Lordships have said this morning, important. Where do they go beyond that? When it says "independent", they are a very independent group of people. Their role is to advise ministers but also to provide advice to the National DNA Database Board—that is a Board that reflects Police Service and Home Office involvement in the DNA Database—to add a level of open public transparency to the questions that are being asked. I anticipate they will be an extremely influential group in helping the database and ministers to manage and meet that balance between prevention and detection of crime and public confidence.

Q123 ***Baroness O'Cathain:*** Surely, part of the problem with the national DNA Database at the moment is that it is selective, as has been pointed out by several of their Lordships today, whereas if it were comprehensive for everybody, like birth certificates, there would not be that problem. Actually, civil rights would probably be better protected by having a national database for everybody compulsorily rather than having a selective approach, which whether it appears that way to you or not, appears that way to a lot of people.
Chief Constable Neyroud: I think there are good cases. In a sense, it is important that it is not me that is arguing that point.

Q124 ***Baroness O'Cathain:*** I understand that.
Chief Constable Neyroud: It seems to me that it is my role to make sure that the one we have is being run effectively rather than to move into that wider sphere.

Q125 ***Baroness O'Cathain:*** Going back to my original question, do you think that this is an area that the National DNA Database Ethics and Advisory Group should take on in order to relieve you of that problem?
Chief Constable Neyroud: It is not just the bioinformation on the DNA database. Of course we also hold fingerprint and other data as well. I think it is an area that they are bound to explore. There is also an area raised in the Nuffield Report on bioinformation used for crime, and it is also an issue that the Human Genetics Commissioner will be exploring over the next period of time. It is bound to be explored. It should be explored. Clearly, it is an issue that Parliament should be doing, not me.

Q126 ***Viscount Bledisloe:*** I just wanted to clear up, going back to the previous question, that I was only advocating the removal of the data after the file was closed, not after the file remained opened but is yet unsolved.
Chief Constable Neyroud: I understood that.

Q127 ***Lord Peston:*** You have largely touched on my question which I think is probably for Assistant Chief Constable Gargan. It is on the influence the NPIA have on these kinds of matters: the use of bioinformation and so on. Have you been influential? Have you been involved?
Chief Constable Neyroud: That is probably a question for me actually. How influential are we? I do hold overall policy responsibility in a number of these areas. Together with ACPO, not the colleague to my right but together with ACPO, we have been seeking to develop a new, forward-looking national forensic strategy. In fact, one or two colleagues behind are responsible for the Police Science and Forensics Unit which is the core of providing advice to Government, answering your questions and making sure that a great deal of information is entered into the public sphere, including things like the DNA Database report, so that the public are able to debate these issues on the basis of that information.
Lord Peston: I apologise. There is a limit to how many acronyms I can take in at one time!

Q128 ***Lord Norton of Louth:*** I suspect this is a question for Mr Gargan because we now come on to RIPA, which you mentioned at the beginning. Various criticisms have been made of the legislation and the way it was drafted, and of course in written evidence there was reference to a position of the bureaucracy on public authorities, which I think you have referred to in opening. Indeed, if I heard you correctly in opening, you said that there is a case perhaps for re-visiting the legislation in its entirety. Would you like to expand on that, both the rationale for it and what you think might come as a result of that?
Assistant Chief Constable Gargan: My assessment and the assessment of the group that I have been working with for quite some time is that the primary fault with RIPA is not so much that it is poorly drafted or structured but rather that it is inadequately explained. Behind the Act came along the explanatory notes but unfortunately they were really no more than a summary of the Act. Then, behind the notes came the codes of practice but, sadly, they were no more than a summary of the notes. There are quite clearly some defects in the legislation from the point of view of ACPO and the Service. For example, there is the insistence that in case of covert surveillance the authorising officer and the applicant should be from the same organisation, the same police force. We are trying to work increasingly on a cross-border basis and that makes it difficult. There is an insistence, for example, that the authorising officer will be a police officer, and we are trying to work increasingly in a world where police officers and police staff work in a more integrated way and that causes us some difficulty. There are difficulties about the rigidity of timeframes and authorisation periods, and there are difficulties around one or two of the specifics of the legislation itself. The most often quoted is the example of the elderly victim of repeated distraction burglaries in their own home and the enterprising local officers want to do the right thing and install a camera. There is a paradox in the Act that states that because it is inside a dwelling, then it must be intrusive surveillance, but because the crime, in many people's interpretation, is unlikely to amount to serious crime, you cannot authorise intrusive surveillance. In previous years, we have had to agree with the Chief Surveillance Commissioner, the

predecessor to Sir Christopher, that we are just going to go ahead and do it because it is the lesser of several evils. There are technical problems around participation which is not placed on a legislative footing. There are technical problems associated with the concept of the Covert Human Intelligence Source—an informant in "old money". The legislation provision covers everything from an undercover police officer dealing with six-month long infiltration deep under cover right the way through to some very cursory contact on behalf of somebody who is doing a bit of work for the Police. The boundary there is difficult. Sir Ronnie Flanagan in his report draws attention to risk aversion on the part of the Police. Unfortunately, one of the consequences of our own cultural risk aversion is that we tend to over-authorise. We have tried to look for sources of advice that would give colleagues the confidence not to over-authorise activity. I have been responsible for that for quite some time. My route into this was a real horror and disappointment when I was a Chief Superintendent in Leicestershire Constabulary. Colleagues were coming to me wanting a 17 page authorisation signed because they wanted to turn round a public CCTV camera on to a parade of shops to watch a few "ne'er do wells" who were breaking the odd window. It was our sense that RIPA was not ever intended for that and that the bureaucracy was senseless. We believe in the highest possible standards for covert policing but let us not dress patrolling activity using overt cameras up as covert policing. Let us apply a little common sense, for example to the case where we send someone into an off-licence and ask him to try to buy four cans of lager so that we can prosecute the shop-keeper if he is selling inappropriately. Let us not dress that up as covert policing. Let us just send them in and not authorise them as covert human intelligence sources. It is applying a sensible level to that. We endeavoured across a range of scenarios—automated number plate reading systems, CCTV, coverage of an intelligence source—to supply a set of principles to the Service that said: here is a starting point and a set of scenarios where we really do not think you should be having an authorisation. Unfortunately, our efforts at the Service to explain RIPA and offer this narrative have been unsuccessful in that whilst we have had the support of the Crown Prosecution Service, HM Revenue and Customs, Prosecutions Office, DPP and ACPO Cabinet, there have been others who have said that that goes too far. The Chief Surveillance Commissioners said that some of the assertions that we were trying to make go too far. We have now reached the point where that has to be handed back to Government because, whilst we maintain this desire for the highest standards, we cannot agree on what is an appropriate level of bureaucracy.

Q129 ***Lord Norton of Louth:*** So the legislation itself then you are arguing imposes certain limits which can limit you in doing your job and I think, from what you are saying, might impose a certain risk-averse culture as well, which gets in the way of a common sense application?
Assistant Chief Constable Gargan: Indeed, and I think the way it has been interpreted is the problem. The solution to this could well come from a re-drafted code of practice. It certainly does, because of the interpretation of the legislation, which is inconsistent because some people will not authorise the sorts of activities that I am describing and will just get on with them. There has never been a case lost in court but others do authorise it. We seek that clarity and chief constables are crying out for that clarity. This week or next week, Trevor Pearce from the Serious Organised Crime Agency and I will be writing to Mr McNulty effectively to conclude the review of RIPA, which we have been doing over several years, and we will hand those issues back to the Home Office with a plea for help.

Q130 ***Lord Norton of Louth:*** I take it from your point that quite clearly, from the evidence you have given, it is not only a problem but an immediate problem; in other words, it is a case not just for change but for fairly quick change. You have said the route through that might be through the code, which would be a quicker way of doing it than primary legislation.
Assistant Chief Constable Gargan: Indeed and cash and time (cash in the form of police officer time) are being wasted on a daily basis at the moment.

Q131 ***Chairman:*** ACPO's evidence mentions proportionality and necessity. I wondered if you could kindly expand on whose responsibility it is to determine proportionality and necessity within the system and what criteria are used to do so.
Assistant Chief Constable Gargan: I think it is a shared responsibility for all of us. At the time of the Human Rights Act being enacted, ACPO urged every police force and every portfolio of area to conduct audits and reviews of every policy to assess their compliance with the Human Rights Act. We continue to audit new policies against Human Rights Act criteria. That shared responsibility is reflected in training, ranging from the initial Police Learning and Development Programme through which every recruit constable passes right the way through to the command course training for future chief officers. It is a feature of specialist training, for example, for firearms commanders for whom this is obviously a very relevant and important set of considerations. And also, as well as training, it forms part of our operational planning. Planners in police forces up

and down the country use a mnemonic which is IIMARCH which relates to Information leading to the operation and the Intention of the operation, the Method by which the operation will be carried out, Administrative considerations, Race and diversity considerations and finally Human rights considerations. So it is risk assessment too. There is this comprehensive process through which each operation passes and part and parcel of that set of considerations is human rights. Of course, it is actually about the people we recruit, the ethos of the Service and the culture of the Service. That is where the human rights considerations really will stand or fall. We are very proud of that culture and that tradition. It is, of course, subject to inspection. Our inspection regime is a very intrusive process. The inspection of the Office of Surveillance Commissioners is not a cosy, fireside chat with a former judge. It is a serious and intrusive exploration of our activity. Obviously the human rights considerations are central to that inspection process.

Q132 ***Lord Lyell of Markyate:*** Going straight on from that, ACPO's written evidence does state that the current supervisory arrangements from these various Commissioners—from Richard Thomas, the Information Commissioner, from the very senior judge who does interception of communications, and likewise the Office of the Surveillance Commissioners—and from what you are saying that they are "inefficient, cause duplication and are anachronistic". Could you just give us some specific examples of the adverse effects that these supervisory arrangements have had on you as law enforcement agencies?

Assistant Chief Constable Gargan: Yes. I should begin by saying that largely there are good relationships with our Commissioners. I received a letter yesterday from the ACPO lead on communications data, Mr Jim Gamble, and he reminded me of the great work that is done between the ACPO Commons Data Group and the Interception Commissioner and what a collaborative approach there has been over the years working with the Surveillance Commissioners. There has been much good work done on a collaborative basis, but the fact of having separate bodies investigating largely the same field of activity creates a bureaucratic cost. It creates cost around the time to prepare. A force in the south-west of England contacted me to tell me how they had literally waved goodbye to the Interception Commissioner on the Friday and the following week on the Monday morning up popped the Surveillance Commissioners for their inspection, and these visits do not just happen overnight. It takes time to prepare them and to assemble the evidence. That was an unnecessary duplication. We find that in the way the Commissioners are set up, you regularly encounter conflicting advice from within the same office, which is unhelpful and confusing to staff, with different Commissioners reaching different conclusions in respect of the legislation, which we acknowledge is of course very complex and cannot be entirely consistent. Worse still, we find conflicting advice between Commissioners. When the ICO is telling a police force one thing and the Office of Surveillance Commissioners is telling it another, and these are relatively junior members of staff receiving that conflicting advice, it can be difficult. An example of that was a force that was visited by the Communications Commissioners and advised to alter their form which was unnecessarily bureaucratic. There was a particular application form and there were too many boxes in it. So they very obligingly combined three boxes into one and that was very much to the liking of the Interception and Communications Commissioners. Sadly, when the Office of Surveillance Commissioners next saw the Part 3 Property Interference Application from that force, they complained that these rather helpfully spaced out three boxes had disappeared and had been replaced with one, and they urged the force to right that wrong as quickly as they possibly could. It is an irritation rather than a substantial problem but the opportunity of having a combined inspectorate that looked across the question of privacy and covert investigation would be an opportunity both for lessening the burden on police forces but also for improving the quality of regulation. We would continue to welcome the fact of inspection, the fact of Commissioners, the fact that they are there, and the fact that they provide us with an opportunity to show that we are serious about being transparent, demonstrating the integrity of our systems and being open to scrutiny.

Q133 ***Lord Lyell of Markyate:*** One can understand the point you make and sympathise with it, but to throw out these bodies which have a very significant task themselves and to try and combine them, is that necessarily the way or could they perhaps co-ordinate between themselves in building up the kinds of questions they are going to ask you? I imagine they give you notice of most of the questions. It would be a major task, would it not, to have one Commissioner to do all this?

Assistant Chief Constable Gargan: The outcome that would be most welcomed by the Police Service is better coherence in our inspection, a reduced bureaucratic burden, a reduced administrative burden and consistency in the advice we receive from our Commissioners. If that could be achieved through better co-ordination, then that is not really a

matter for us. We articulate the problem and offer this as a possible solution.

Q134 ***Lord Lyell of Markyate:*** If you have one leaving on the Friday and the next one coming on the Monday and they knew this was happening, they probably could have co-ordinated?
Assistant Chief Constable Gargan: Indeed, and we would very much welcome it had they done so.

Q135 ***Lord Rowlands:*** Have any of these Commissioners produced a seriously critical report of any of the forces?
Assistant Chief Constable Gargan: Oh, yes, the Office of Surveillance Commissioners has been particularly critical of several forces.

Q136 ***Lord Rowlands:*** What has been the nature of the criticism?
Assistant Chief Constable Gargan: There are two types. At the outset, the nature of the criticism was about the way that the application process was managed. A lot of forces were criticised about the absence of effective training in the period following the enactment of RIPA. Then subsequently there has been some criticism around the way that it is being interpreted and the work of the ACPO group. This relationship with the Chief Surveillance Commissioner and the Office of Surveillance Commissioners has not always been one of entire agreement and forces that have followed the advice of the ACPO group that I chair have, on occasions, risked criticism from the OSC. I have had two or three local authorities who reported having been visited by one inspector from the Office of Surveillance Commissioners in one year and faced criticism about their way of operating; they then changed it and when the inspector comes around the next year, they face criticism for not being more like they were previously.

Q137 ***Lord Rowlands:*** Most criticisms have been procedural rather than fundamental in terms of the issue of liberty and the individual?
Assistant Chief Constable Gargan: Yes.

Q138 ***Lord Rowlands:*** They have not made any criticisms regarding issues of liberty?
Assistant Chief Constable Gargan: No, because most issues of liberty are considered at the time of application. Because of property interference and intrusive surveillance, the Commissioners play a very important role on an application-by-application basis. That is where that side of it is looked at. It is more the administrative set-up, training, record-keeping, security processes and the accreditation that is looked at during inspection.

Q139 ***Baroness O'Cathain:*** On this issue where you have three individual organisations and you are subjected to these types of investigation by these three groups of people, first, do you have the scheduled responsibilities of each of the three organisations? Secondly, have you analysed it to see if there is any duplication like comments on training, and, if so, is it comments on training on certain issues which are covered by all three? It might help this Committee if you could, and I am sure you have done something because you have obviously got this information at your fingertips and right up there in your head, give us some sort of a résumé of where the real problems lie or even a statement of what the responsibilities of each of the three are so that we could look at it and see. It is in every area; it is not just in the Police Force. In every area of business in this country we have the same sort of problem. Usually it is little empires, and it is so much better to have a big empire and have departments looking at the specifics. I wonder if we could get that sort of information.
Assistant Chief Constable Gargan: There has been some work done. It is incomplete but I am happy to take that away and to offer a paper to the Committee. Of course I should emphasise two points. The first is that the Information Commissioner's powers and inspection powers are very limited. There is a debate about whether there should be more. Were there to be more, then that would add to the issue that I am describing to you. The second point that I would make is that of course it does not stop with the OSC Interception of Communications Commissioner. We also have Her Majesty's Inspectorate of Constabulary that recently completed an inspection about covert technical capability, and others are interested too from time to time. I would be happy tell you.

Q140 ***Baroness O'Cathain:*** Can you chuck them all into the box?
Assistant Chief Constable Gargan: Yes.

Q141 ***Lord Morris of Aberavon:*** Are there inherent dangers in combining these various bodies? We would all be in favour of reducing bureaucracy and saving money or whatever. Is not the advantage of having different persons making the reports that one or other might be more radical in their suggestions? I am currently reading *The Life of Sir Robert Peel*, which may encourage you. There always has been an argument against a national police force. That is a simple argument I suppose for combining each of these three independent bodies.
Assistant Chief Constable Gargan: They may be more radical the one and the other. They certainly, as I have tried to get across this morning, do approach these issues from different perspectives already.

Q142 ***Lord Lyell of Markyate:*** ACPO suggests that citizens could benefit if the Investigatory Powers Tribunal were better marketed and understood. I suspect most citizens have never heard of the Investigatory Powers Tribunal. Can you explain a little bit how citizens might benefit and what happens?
Assistant Chief Constable Gargan: It is important to repeat the point—and I apologise for doing so—that these techniques are vital to the Police. Covert techniques are fundamental to what we do. We know that in order for us to be able to continue to use these techniques, we need to prove ourselves trustworthy. Therefore, we seek opportunities to show that we apply the highest professional standards and that we deserve the trust that the community places in us to carry out covert investigative techniques. Anything that is out there that will assist in demonstrating our transparency, that will assist in demonstrating our integrity, the integrity of our systems, and that will offer a redress to those who feel that they have been wrongly treated by what we do or may have been wrongly treated, anything that addresses those three themes along with the theme of compliance with human rights and with the legislation, is very welcome. If you have something that is expressly designed to do that and provide that reassurance and yet very few people know about it, it seems to represent a missed opportunity. Several Police forces contributed to this submission which I have edited on behalf of ACPO, and more than one made the point that we would be very happy to encourage that greater scrutiny.

Q143 ***Lord Lyell of Markyate:*** How many cases a year come before the Investigatory Powers Tribunal?
Assistant Chief Constable Gargan: I do not know. I was speaking to the Serious and Organised Crime Agency the other day and apparently what happens is that when somebody writes in to the tribunal that they suspect they may be the subject of surveillance, the tribunal will send out to organisations to ask who may or may not be active against a particular individual. There are two particular categories of people of whom we are quite wary. One is the criminal who might want to know whether they are being surveilled by the police, and there is a potential usefulness to them in knowing that. The second is some people who are potentially mentally disordered and they feel that they perceive things that the rest of us would perhaps not perceive, and that is not limited to police surveillance but alien surveillance and other categories too. In terms of the work out of the tribunal, I am not aware but I believe that there has only ever been one publication of a tribunal finding since its inception, and I cannot even give you a memorable name, I think it is the case of *C*.

Q144 ***Lord Lyell of Markyate:*** Why do you say it should be better marketed? It sounds as though there is nothing to market?
Assistant Chief Constable Gargan: Perhaps the issue is that the Tribunal ought to be encouraged to be a more publicly visible facility both in terms of encouraging people to use it and, where meaningful claims have been made, to actually publicise those findings so as to reassure the community that they are being protected and we are using our powers responsibly.

Q145 ***Lord Rowlands:*** If we can turn to CCTV. Before I ask a question about the National CCTV Strategy, could you perhaps clarify exactly where we are on the effectiveness of CCTV? I ask that because I do not know if you have had a chance to read any of the previous evidence given to us, this is Professor Norris and co., who in a series of exchanges said that the Gill study said in 2004 that CCTV had very limited impact in reducing fear of crime and quotes another one, the Ditton team in Glasgow, who found crime increased when CCTV was introduced, and then Farrington and Walsh said it would be better spent on more street lighting. Where do you stand on the assessment of the effectiveness of CCTV?
Deputy Chief Constable Gerrard: It depends how you define the word "effective". Certainly a lot of the academic research would tend to suggest that in relation to reducing crime then it has mixed results. It certainly has mixed results in terms of town centres where a lot of the crime is alcohol related. Before CCTV can effectively deter people (a) they need to know that the cameras are there, (b) they have got to be thinking rationally and about the consequences of their behaviour, and (c), the CCTV needs to be able to summon an appropriate response because if it does not then it is a little bit like somebody stood on a street corner watching you but doing nothing about it and in the long-term it might not deter behaviour. The evidence and academic research that I have seen says it is very effective in places like car parks where offenders are going out specifically to break into cars and are thinking rationally and about the way they are going to do it, but in terms of our town centres, where a lot of the behaviour is violent or disorderly behaviour, often fuelled by alcohol, people are not thinking rationally, they get angry and the CCTV camera is the last thing they think about and even the presence of police officers does not deter them from fighting and being disorderly in the streets, so cameras are not likely to. In terms of reducing crime there are mixed results and I fully accept that. The research in terms of reducing the fear of crime, if you look at Professor Martin Gill's research study from the Home Office, he said there was some quite good indication that it reduces the public's fear of crime. If

you look at where most of the pressure is for CCTV in the community, the vast majority of it comes from the public who actually want it within their local communities. It is certainly not being driven by the Police Service, it is actually being driven by the local communities. I think some of them then get disappointed when the CCTV goes in, and Martin Gill's research tends to suggest that, because they have high hopes for it and because it does not deter as much crime as they thought it was going to do—

Q146 ***Lord Rowlands:*** Do you think the public can sometimes get misled on the benefits of CCTV?
Deputy Chief Constable Gerrard: I think the public may have a different expectation in terms of the amount of crime that CCTV might prevent.[1] The principal measure of effectiveness as far as the Police Service is concerned is in relation to the support of the investigative process. When a crime has occurred CCTV is a vital element of the investigative process. It is not an understatement to say now that the first piece of evidence that an investigating officer will go looking for is the CCTV evidence. The first investigative action very often is secure all available CCTV evidence. Interestingly, there is very little academic research on the effectiveness and usefulness of CCTV in the investigation of crime, most of it is focused on does it reduce crime, not what is the impact of it in terms of investigating crime. You only need to watch the television on a daily basis and to read the media on a daily basis to see how many crimes are detected, or certainly the investigation greatly assisted, as a result of CCTV evidence.

Q147 ***Lord Rowlands:*** I was interested because it was implied in part of your evidence that you do not collect evidence of how CCTV is being used in the investigation of crime in a thorough and comprehensive way whereas I noticed the Chief Constable on DNA said that you measure success rates by the use of data. If that is the basis of the case for putting so much investment into CCTV, why are you not collecting what would be obvious evidence?
Deputy Chief Constable Gerrard: We are in the process of doing that. We were required through Her Majesty's Inspector of Constabulary and the Police Standards Unit to justify the expenditure around DNA fingerprints and in order to do that we are required to record the amount of crimes that are detected, both primary detections and secondary detections, offences taken into consideration, that come from both fingerprint and DNA. There has been no requirement on the Police Service to do that in relation to CCTV.

[1] *Note by witness:* The witness wished the record to reflect that he meant that "the public may have a different expectation in terms of the amount of crime that CCTV might prevent".

Q148 ***Lord Rowlands:*** There has been large investment.
Deputy Chief Constable Gerrard: The investment, interestingly, has not been made by the Police Service. If it had been made by the Police Service I suspect Her Majesty's Inspector of Constabulary would be asking what we had done with the money. The vast majority of public space CCTV is owned, monitored and run by local authorities. They are, understandably so, crying out for some information that supports the effectiveness of it and I would dearly like to provide that to them, and one of the recommendations within the National Strategy is that the Police Service do exactly that. My view is that we are unlikely to persuade government to invest further in CCTV if we cannot show the effectiveness of CCTV. The Martin Gill research study that the Home Office sponsored was an attempt to do that but it did not ask the right questions. All it did ask was ask "how much crime does CCTV reduce or prevent" rather than "how effective is CCTV in the investigation of crime". It is very difficult to put a cost on it but several years ago London was suffering from a nail bombing campaign by an individual by the name of Copeland and his avowed intention was to start a race war. He was targeting specific parts of London with his nail bombs and there were extremist groups claiming responsibility for the actions. That event was entirely supported by CCTV evidence in terms of actually detecting that crime. What value do you put on the price of that detection? How do you start to value those sorts of things?

Q149 ***Lord Rowlands:*** You are doing it in the case of DNA so presumably there is a methodology you can apply.
Deputy Chief Constable Gerrard: There is a methodology in terms of counting the detections. We had the same issue with the recent situation in terms of the bombings of London, what value does society put on those detections, and that is an issue right across the board in terms of detecting crime. We are in the process of developing our system of counting the number of detections where CCTV assists. I am of the view, and from limited research we have done in my own force area, we get more detections from CCTV or CCTV assisting in the detection of crime than we do from fingerprints and DNA combined.

Q150 ***Lord Rowlands:*** You did mention the National CCTV Strategy and there are 44 recommendations in that Strategy. Can you give us some order of priority and how are you going to carry it forward?
Deputy Chief Constable Gerrard: As a co-author I think all 44 are very important, but I would say that, wouldn't I? The Strategy was written as a result of a concern that I had, that I expressed through ACPO

that then went on to the Home Office, that we have probably the most extensive public CCTV surveillance network in the world, we are the envy of many governments and certainly the envy of most police forces in the world. Most of them cannot understand how it has happened and why the British public and the British Government have allowed it to happen, and they cannot understand how we have managed to get it in place. But, despite having a very extensive CCTV network, it has been developed in a piecemeal way, it has been developed in a relatively un-coordinated way, and we are not making maximum use of its effectiveness. As the technology changes it is a significant issue for everybody involved right the way through the criminal justice system to play catch-up. My colleagues in the courts, for example, are still just getting over the development of VHS recorders where the rest of us are looking at the next development past digital and DVDs, Blu-ray and all sorts of stuff like that. There is real potential for a massive waste of money if we do not co-ordinate this together. My number one priority would therefore be some sort of national body, and it is a recommendation, around managing this whole approach and co-ordinating the whole approach of public CCTV in this country because without it we have every local authority doing their own thing, every police force trying to catch up with every local authority doing their own thing, every CPS Service, every Probation Service, every magistrates' court, crown court and defence solicitors all trying to get behind somebody else's bit of technology. At the moment I am taking perfectly good digitally recorded CCTV evidence and putting it on to an old-fashioned VHS cassette to allow it to be played in some parts of the criminal justice system at significant cost and degradation of the quality of the image. It cannot go on like that. I think we need some form of national co-ordination board. Secondly, if I am allowed three, it is around driving out some standards. At the moment we are faced with hundreds and hundreds of digital imaging formats. It is a bit like the current argument they are having about Blu-ray and HD DVD, but if I turn it back a bit it is like VHS and Betamax. If you can imagine instead of having VHS and Betamax, add another 400 different formats. My police officers can go out and recover CCTV and find it in any one of those 400 formats without the necessary playback software available. What used to be a very simple and straightforward task for us to recover CCTV evidence, which was to go and get the VHS cassette and put it in the police station, is now becoming quite a technical process and the Police Service is having to move towards employing people with technical expertise just to get the evidence and that is because there are so many different formats out there. If this is CCTV that public money is being spent on I would like some form of standard so it is compatible right the way through the process. Finally, there is no point having standards if they are not enforceable so that requires some form of mechanism. We talk about appropriate legislation but it might be just tightening up some of the existing codes of practice and some inspection regime that says to people, "This is what we require of you". Every time you see a poor quality CCTV image it is not fit for purpose and if it is not fit for purpose it does not comply with the legislation which covers it, which is the Data Protection Act, and that is not being effectively policed. The Police Service and the criminal justice system is wasting a huge amount of time on trying to manage and recover CCTV that is inappropriate, we are missing detection opportunities and that needs to be dragged together.

Q151 ***Lord Rowlands:*** You say somewhere in your evidence that the vast majority of cameras are in the private sector anyway, is that right?
Deputy Chief Constable Gerrard: Yes.

Q152 ***Lord Rowlands:*** If so, have you got any recommendations on how you relate the public sector CCTV systems with the private sector?
Deputy Chief Constable Gerrard: That is the difficulty. In fairness to my colleagues in the public sector, in the main their systems are pretty good because they work fairly closely with us, but we are duty bound to gather evidence from wherever we can, so we are duty bound to gather evidence if it is available, and very often the evidence that we gather does not relate to the premises that we gather it from. It might be an assault in the street and the CCTV system from a shop has captured that assault in the street, so we are asking them to provide us with the CCTV evidence to help prove an investigation or support an investigation that is nothing to do with them. We are in a bit of a dilemma. On the one hand, we do not want to dissuade them from providing us with the CCTV evidence but, on the other hand, we would dearly like them to improve the quality. There is a dilemma around how we drive up the quality of CCTV in the private sector. Bear in mind that could also comply with the Data Protection Act in most cases and if that was properly enforced we perhaps could do it that way.

Q153 ***Lord Peston:*** In my judgment, I think Deputy Chief Constable Gerrard has anwered my two questions when he was talking to Lord Rowlands, but could I just make sure I understand his answer to the last of the questions. You seemed to say that you

do favour a national body to regulate all this, number one, and, secondly, you seemed to say you think it ought to have real powers to make sure it gets its own way. Did I rightly interpret what you were saying as that?

Deputy Chief Constable Gerrard: Certainly a national body to co-ordinate the development of CCTV in the UK and to make the most of the significant public investment we have already put in. When the money originally went out, it went out to lots of local authorities and at that stage none of the local authorities had any expertise around the development of CCTV, although they have it now. We do need to better co-ordinate. Certainly a national body to co-ordinate and then some form of legislative support or increased powers perhaps for the Information Commissioner's office to drive up the standards of CCTV, not just in the public sector but the private sector so that the CCTV that we are taking is appropriate. At the end of the day if the public think the camera is there they should expect the camera to do the job at least. If we are going to the trouble of taking pictures of people they should be fit for purpose otherwise it is a double-whammy against the public, is it not, you have conned them into thinking that they are being covered by CCTV but the images are not any good. We need some way of driving up the quality of the images.

Chairman: Gentlemen, on behalf of the Committee can I thank you very much indeed for your attendance and the evidence you have given. Thank you very much.

Supplementary letter from Sir Paul Kennedy, Interception of Communications Commissioner's Office

I write to you in your capacity as chairman of the Select Committee on the Constitution, and in relation to the evidence heard in public on 16 January 2008 in relation to the surveillance society. I am concerned in particular with the evidence given to you by Assistant Chief Constable Nick Gargan because I fear that it may have mislead your committee in certain respects. I invite you to look again at the answers given to questions 128 and 133 inclusive, and then to read the enclosed copy letter from Mr. Gamble to ACC Nick Gargan dated 14 January 2008. In his evidence Mr Gargan did refer to that letter when answering Q132, describing Mr Gamble as "the ACPO lead on communications data" but so far as I can ascertain you were not shown the letter, and thus were not able to see for your self the contrast between the tone and content of the evidence that you received. As you can see the letter is not protectively marked, and it was side-copied to me, so there is no difficulty about my drawing it to your attention.

In relation to the answers themselves I would like to make four points, namely:

1. Codes of Practice

I found it surprising to see the Codes of Practice described in answer to Q128 as "no more than a summary of the (explanatory) notes". The Codes are the product of a lot of liaison work involving members of staff of the Home Office, the Data Communications Group and my office, and the object was to ensure that they meet the needs of law enforcement agencies and other agencies entitled to acquire communications data. Changes were made to enable forces to streamline their systems, to eliminate bureaucracy, and to speed up collection of data, and, as is clear from Mr Gamble's letter, my inspectors have been encouraging police forces to take advantage of the changes.

2. Duplication in Preparation

In answer to Q132 Mr Gargan said that "having separate bodies investigating largely the same field of activity creates a bureaucratic cost; it creates cost around the time to prepare". I find that difficult to understand, because the activities being considered by the representatives of the Office of Surveillance Commissioners (OSC), and those being considered by the Inspectors from my office are different. My inspectors are looking at the collections and use of communications data. Most of their time is spent in the Single Point of Contact Office, so the preparatory work cannot be the same as that required for a visit by the OSC. If the two visits were to coincide it would simply mean two lots of preparatory work would have to be done at the same time. There would not be less preparatory work, and the impact of the combined visits would be greater.

3. Timing of the Inspections

In the answers to Q132 it is asserted that there is a lack of liaison between the OSC and the IOCCO in relation to the timing of visits. "A force in the South-West of England (unspecified)" is said to have contacted Mr Gargan to tell him that having waved goodbye to my Inspectors on the Friday, on the following Monday "up popped the Surveillance Commissioners for their inspection". No date is given as to when this occurred, but the impression created is that it could happen anytime. In fact the OSC prepares an annual inspection programme for the year beginning in April. It is supplied to my Chief Inspector in the preceding January. He then prepares quarterly plans for the IOCCO Inspectors which ensure that police forces and other public bodies do have breathing space between inspections. He is not aware of any recent occasions when IOCCO and the OSC inspections were back to back. It may have happened as a result of re-scheduling or some exceptional circumstances, and inspections have been re-scheduled when the police forces have asked for more time to prepare, but the impression given by the answer to your questions is not only erroneous, it is also offensive to those taking care to ensure that there is proper liaison in relation to the timing of inspections, as you would expect.

4. Conflicting Advice

A large part of the answer to Q132 is devoted to a complaint that the police force receive conflicting advice. It is said, as a general proposition, and without any specific examples, that "you regularly encounter conflicting advice from within the same office, which is unhelpful and confusing to staff". I simply do not know what lies behind that observation. My Inspectors operate out of an office which is entirely separate from that of the OSC, so is the suggestion that my inspectors are not advising consistently with each other? If so I find that difficult to accept for three reasons—first, the normal practice is for the same Inspectors to inspect and re-inspect the same police force. Secondly, the Inspectors do liaise and meet regularly, and, thirdly, both the Chief Inspector and I read every inspection report which is issued, so I know that a consistent approach is maintained.

Furthermore it has never been suggested to anyone in my office that the Inspectors have been giving inconsistent advice, Mr Gargan refers to "different Commissioners reaching different conclusions in respect of the legislation," and to "conflicting advice between Commissioners". I do not know whether I am one of the Commissioners concerned, but I am aware of only one occasion when the IOCCO and the OSC have had any difference of opinion as to the impact of the legislation. Sir Christopher Rose and I have been in correspondence about that, and we hope to be able in due course to reach agreement as to what the legislation requires, but the difference of opinions in relation to complex legislation is of interest only because it is unique. Mr Gargan complains of the IOCCO telling a police force one thing and the OSC telling it another, and gives an example of my Inspectors advising a police force to alter their form on the basis that the form in use was unnecessarily bureaucratic. That I can accept. I regularly see inspection reports encouraging the use of the new Home Office form which is available on line and is much less bureaucratic. Apparently the police force which Mr Gargan had in mind regarded the advice of my Inspectors as an invitation to amend the form which they used for a Part 3 Property Interference Application and the OSC were unhappy about that. Whether they were right or wrong to disapprove it is not for me to say, as neither I nor my Inspectors have any jurisdiction in relation to Property Interference Applications, but we will continue to urge all police forces to use the least bureaucratic means available to comply with the requirements of the law in relation to the parts of the statute with which we are concerned.

So that they may be aware of the fact that I have written to you I am sending copies of this letter to Sir Christopher Rose and to Mr Gargan.

14 February 2008

Annex 1

Letter to ACC Nick Gargan, Thames Valley Police from Jim Gamble

14 January 2008

Dear Nick

SELECT COMMITTEE ON THE CONSTITUTION: A SURVEILLANCE SOCIETY

I refer to the above and your attendance before the House of Lords Select Committee on Wednesday 16 January 2008.

A circulation sent out by your staff officer Liz Kirk states you are to give evidence before the committee and that you are looking for practical examples of the impact of inspections undertaken by the Interception of Communications Commissioner's Office (IOCCO) regarding compliance with Chapter II of Part I of RIPA.

The Data Communications Group (DCG) and Home Office has for several years had a positive working relationship with the Interception Commissioner (Sir Swinton Thomas and more recently Sir Paul Kennedy) and the team of Inspectors who undertake inspections of the public authorities, which includes police forces.

The DCG, Home Office, the Commissioner and his Inspectors hold regular meetings to discuss inspection and policy issues and ensure that we are synchronised in mutual areas of work.

IOCCO inspection reports are shared with the Home Office and, where training issues are identified by an inspection, with the DCG.

There have been other positive outcomes from our joint work with the Commissioner and his Inspectors such as the:

— streamlining of the application processes now included in the new code of practice (implemented in October 2007);

— development of a simple application and authorisation form; and

— setting down guidance for applicants and authorising officer so as to simplify what should included within applications and authorisations.

DCG has had positive feed back from the police forces concerning the inspections by IOCCO, especially as the Inspectors have been very proactive in encouraging police forces to use the streamlining processes contained within the new code and the simplified forms.

Parliamentarians may well want to reflect on whether a single administration supporting the work of various Commissioners will bring about a more effective regime and that is to be encouraged.

Should you wish to discuss these matters further please do not hesitate to make contact with me directly.

Yours sincerely

Jim Gamble

Further supplementary letter from Nick Gargan, Assistant Chief Constable, Association of Chief Police Officers (ACPO) to Sir Paul Kennedy, Interceptions Communications Commissioner

I am grateful to you for sending me a copy of your letter to Lord Goodlad dated 14th February 2008. Your letter indicates that my evidence may have misled the Constitution Committee. As you can imagine, the suggestion that I may have misled a Parliamentary Committee causes me great concern. The evidence was prepared with great care and I have subsequently re-visited it with equal care. I maintain that it is sound and accurate, but would happily offer some clarifications in the light of your letter.

Preparing the ACPO Submission

When the Committee published its call for evidence, it was agreed that I would be responsible for pulling together a response on behalf of ACPO. The submission was based on the Review of RIPA, several surveys that have been conducted in recent years and was further informed by contributions from a number of police forces and relevant ACPO Lead officers. Although Jim Gamble, Chair of the ACPO Data Communications Group, did not send a contribution to the submission, he did write to me immediately prior to my evidence as you point out. So important was his contribution that I referred directly to it during evidence. I thought that I had done justice to his positive comments about your relationship, but acknowledge that I could have said more and could, indeed, have submitted his letter to the Committee. That said, the Committee did impose a strict limit on the size of submissions: a limit that I had already exceeded by some margin!

Your letter makes four principal points:

1. *Codes of Practice*

To the best of my knowledge, there are four Codes of Practice to the Regulation of Investigatory Powers Act 2000. My reference was to the Code of Practice in respect of covert surveillance which was, I believe, first published in 2002 and which was the subject of close scrutiny during the Review of RIPA. All the examples that I gave in evidence to the committee, relate either to that code or to the code in relation to Covert Human Intelligence Sources. That the surveillance code is no more than a summary of the explanatory notes was never seriously disputed during the Review of RIPA or, to the best of my knowledge, since.

You are absolutely right to say that the Code of Practice in relation to the Acquisition and Disclosure of Communications Data is very different and my description does not fit it at all well. Indeed, I received several drafts of the Communications Data Code of Practice as it was being developed and it was often said that the emerging document was successfully avoiding the pitfalls into which its surveillance predecessor had fallen.

In the pressurised environment of the committee room, as I attempted to present the key issues in this very complex arena, I readily acknowledge that I failed to be precise about which Code of Practice I was discussing. I apologise for this omission and am happy to offer that clarification now.

2. *Duplication in Preparation*

The ACPO submission has been directly informed by a survey of police forces, but indirectly informed by earlier survey work as well as many contacts with individual officers of all ranks from many police forces. Although I acknowledge that you find my assertions difficult to understand, they represent a strongly held and often repeated viewpoint of many senior practitioners. Of course, IOCCO and the OSC form only a small part of the broader inspection and accountability framework that exists around policing and it may be that each individual Inspectorate function perceives its demands to be specific, unique and entirely reasonable. My findings offer a different perspective: that of the user. The ACPO proposal does not suggest that the OSC and IOCCO should arrange for their visits to coincide—rather it proposes that there is scope to rationalise overlapping Inspectorate functions which would enable one team of Inspectors to review a somewhat broader sphere of activity: meaning one interview with the Head of Crime, one interview with the Chief Constable, one week of visitors around the headquarters' site, etc. My answer to the Committee's question 133 readily acknowledges that there may be other ways of achieving this.

3. *Timing of Inspections*

As with the question of "duplication in preparation" above, this response was again based on the feedback from police forces. I am sorry that you think my remarks may be offensive to those who are attempting to organise inspection timetables. I have no doubt they do a very good job. The ACPO point was only ever that the fact of two inspections, whether they be separated by six days or six months, is an unnecessary bureaucratic burden.

4. *Conflicting Advice*

The issue of conflicting advice has been one of the most frequently raised with me since I began work in this arena. There are examples of conflicts between individual Commissioners (in this case I mean generally Surveillance Commissioners) that have been the subject of frequent comment to me, in addition there have been many examples of discrepancies between individual OSC Inspectors and indeed between OSC Inspectors and their Commissioners. This may be what prompted Sir Christopher to make the following observation at paragraph 5.6 of his last annual report:

> "Furthermore, views expressed by my inspectors during inspections should not be given undue weight. Although they are better informed than most and have unrivalled experience in comparing how covert activity is carried out by many hundreds of different authorities, they do not possess legal qualifications. Accordingly it would be unwise for any authority to rely on views expressed by my inspectors unless and until their reports are endorsed by me. I have now placed a disclaimer to this effect on all reports."

You acknowledge that there is one (unique) area of disagreement between you and the Chief Surveillance Commissioner but do not say what it is. I can point to a recent operational example from my own force which may or may not be the one to which you allude. In our case, we have received advice from your office that when the police have seized a mobile telephone and that telephone receives a text message or a voicemail, this can be accessed generally without recourse to an authorisation under RIPA. Staff in our Central Authorities Bureaux have been advised by the OSC that to do so would be an interception and therefore would require the authorisation of the Secretary of State. This is just one example, but the cumulative impact of individual tips, hints and pieces of advice from inspectors, Commissioners, administrators and officials from the IOCCO, OSC, and even, on occasion, the Information Commissioner, is confusing to my colleagues in Central Authorities Bureau. Your letter concludes with an example of the sort of confusion that this creates. It is not untypical. That is why ACPO have suggested some changes.

CONCLUSION

In establishing the Covert Investigation (Legislation and Guidance) Steering Group and Peer Review Group, ACPO has attempted to reduce confusion by at least attempting to bring police forces together to try and pursue common approaches to this very complex piece of legislation. We have made much progress and the guidance document (Guidance on the Lawful and Effective Use of Covert Techniques) has moved us forward a very long way. We have written to the police minister, Tony McNulty, highlighting areas where we have been unable to agree on common approaches and hope that he will be able to promote continued efforts to achieve reductions in unnecessary bureaucracy without compromising the highest professional standards in covert investigation. I have now left the Covert Investigation (Legislation and Guidance) Peer Review Group to become ACPO Portfolio Lead on Intelligence within Crime Business Area. The Chair of the Peer Review Group has been taken on by ACC Suzette Davenport from West Midlands Police. She will continue to pursue consensus, whilst ensuring the voice of the Police Service is heard. I hope that my letter has helped to clarify the evidence I gave and hope also that you will be able to work with her to achieve the highest professional standards in the least bureaucratic way in the future.

I am copying this letter to Lord Goodlad, Chairman of the House of Lords' Select Committee on the Constitution and to Sir Christopher Rose, Chief Surveillance Commissioner.

25 February 2008

Further supplementary letter from Suzette Davenport, Assistant Chief Constable, Association of Police Officers (ACPO)

I write to you in my capacity as the newly appointed ACPO lead for the Covert Investigation (Legislation and Guidance) Peer Review Group having taken over this role from ACC Nick Gargan who has given evidence to the above committee. As such any future responsibility for answering further questions raised by the committee falls to me. My understanding is that following the verbal evidence given by my colleagues on Wednesday 16 January 2008 two additional questions have been asked of ACPO concerning the inspection regimes around surveillance and data communications. My response to these questions covers the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioners Office (IOCCO) and HMI constabulary (HMIC). The Information Commissioner's Office (ICO) is not included as they have a purely enforcement role although their remit may be extended to include inspections at some future date.

1. *Are the terms of reference clear in legislation, and do these differ from their websites or published guidance?*

The legislation that provides the appropriate inspection powers for the OSC and IOCCO can be found in Part III of the Police Act 1997 (OSC) and the Regulation of Investigatory Powers Act 2000 (OSC and IOCCO). The Codes of Practice relating to the relevant legislation also outlines the role of the ICO and IOCCO. Her Majesty's Inspectors of Constabulary are appointed by the Crown on the recommendation of the Home Secretary and report to Her Majesty's Chief Inspector of Constabulary (HMCIC) who is the Home Secretary's principal professional policing advisor. The detail of legislated remit and publicised roles and function are outlined at appendix 1 for each of the above inspectorate bodies.

In relation to the OSC, their authority within the relevant legislation is defined as to "keep under review the performance of functions" (Police Act 1997) and to keep under review "the exercise and performance, by the persons on whom they are conferred or imposed" (RIPA 2000). The Codes of Practice outline their remit as "to keep under review (. . .) the performance of functions" under the relevant Acts. Therefore the legislation appears to provide a wide authority that is generic rather than specific. Any specific Terms of Reference from the Prime Minister to the Chief Surveillance Commissioner (CSC) is not something ACPO would be privy to and would have to be requested from Sir Christopher Rose.

The OSC Procedures and Guidance (2006) and Annual Report (2006–07) provide more detail about the inspection process. They describe "oversee operations" and "at inspections all aspects of covert activity are examined and the findings reflect the evidence". The web site is more detailed and includes a fuller outline of the inspection process (list in Appendix 1). The inspection process as outlined by the OSC and carried out in practice easily fits into the broad definition of their legislated role and purpose.

The IOCCO has a similar legislative remit to that outlined above for the OSC. It is a broad authority to "keep under review the exercise and performance of . . ." (RIPA). However the Codes of Practice provides more detail in "whose remit is to provide independent oversight of the exercise and performance of . . ."

and further states that reports to the Home Office may be used to "promulgate good practice and help identify training requirements". Their annual report (2006) reaffirms the IOCCO role as to keep under review "functions" and "the exercise and performance of". The remit of the IOCCO as described within the Act, Codes of Practice and Annual Report is therefore consistent. There is no web site.

HMIC also inspect covert policing methods. Whilst there is no legislative authority to refer to there is a clear outline of the relevant inspection protocol on their web site. The inspection regime covers leadership, strategic framework, tactical response and outcome in the relevant areas under scrutiny. The web site does state that the inspection does not include detailed questions on matters subject to oversight by independent commissioners.

2. *Can we find any evidence of any of them exceeding their remit during inspections eg questions above and beyond?*

As discussed above the legislated remit for both OSC and IOCCO is a broad concept within which it could be argued that all inspection questions or probing is relevant and included unless they were to step entirely outside of surveillance, interception of communications or CHIS matters. Whether these inspection regimes operate within any terms of reference that might be provided to them by the Prime Minister is a separate matter and not one that ACPO is in a position to comment upon. Without this knowledge I would assert that difficulties arise because there is a difference of opinion on the inspection content. The police service has a view that the inspection should be around lawful compliance and best practice to achieve that compliance but there is some evidence that the inspections stray into operational issues such as staffing levels, structure and volume of authorities which the police service believe is beyond their remit.

My view is that HMIC has the primary authority to inspect the function of covert policing as a whole and report on the operational effectiveness of the force in question in this respect. However whilst the web site states they do not include detailed questions on matters subject to oversight by independent commissioners the actual inspection protocols include "examination of authorisation records" in relation to surveillance and "examination of the register" in relation to CHIS. Perhaps unsurprisingly the list of areas covered within the OSC inspection (appendix 1—web site) is very similar to that contained in the HMIC inspection protocol for covert policing methods.

Conclusion

The effect of this is that there is much overlap between inspection regimes albeit they take a different perspective from the information they glean. Any legislative authority is broad enough to be subject to varied interpretation but there is no evidence to suggest any inspection has strayed beyond covert policing issues and within their particular legislative area. Any issues that have been raised, from the policing community, concern "operational policing" matters which is felt to be the prerogative of HMIC rather than the OSC or IOCCO. HMIC have a linked programme of inspections generating greater understanding of the organisation as a whole and the operational interdependencies of distinct functions. I would also like to comment that whilst not detailed above some of the functions of the inspectorates under RIPA also fall within the remit of the Intelligence Services Commissioner and with the growth of joint operations and mutual assistance this can only serve to complicate matters further.

I would like to thank you for the opportunity to look at these issues further and feel that greater clarity around the remit of each inspection regime can only be of benefit both in terms of efficiency and in avoiding any misunderstandings around role, function and remit.

28 April 2008

APPENDIX 1

Office of the Surveillance Commissioner

Legislation

1. The Police Act 1997 s107 provides that:

> S107(1) "The Chief Commissioner shall keep under review the performance of functions under this Part".
>
> S107(2) "The Chief Commissioner shall make an annual report on the discharge of his functions under this Part to the Prime Minister and may at any time report to him on any matter relating to those functions".
>
> S107(5) "Any persons having functions under this Part, . . ., shall comply with any request of a Commissioner for documents or information required by him for the purpose of enabling him to discharge his functions".

The above functions would include the following:

> The scrutiny of authorisations is covered in s96(4) "Where a notice is given to a Commissioner under this section, he shall, as soon as is reasonably practicable, scrutinise the notice".
>
> Authority to "quash that authorisation and order the destruction of any records relating to the information obtained" under s103 (1–9).

2. Regulation of Investigatory Powers Act 2000 provides that:

> S62(1) "The Chief Surveillance Commissioner shall (in addition to his functions under the Police Act 1997) keep under review "the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Part II".

3. Covert Surveillance—Codes of Practice provides that:

> Section 7—Oversight by Commissioners states that "the 1997 and 2000 Acts require the Chief Surveillance Commissioner to keep under review (. . .) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police".
>
> S7.3 states "This code does not cover the exercise of any Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions".

OSC Procedures and Guidance—(Oversight arrangements for covert surveillance and property interference published September 2006)

Paragraph 1.3 states "The OSC is a non-Departmental Public body (NDPB) which was established to oversee covert surveillance and property interference operations carried out by public authorities".

Paragraphs 1.4 and 1.5 detail the daily duties of Commissioners as to "oversee operations" under the relevant Acts and "consider notifications of authorisations".

OSC Annual Report—2006–07

Paragraph 5.5 states "At inspections all aspects of covert activity are examined and the findings reflect the evidence from a small random sample of documentation and interviews of management and practitioners".

Paragraph 7.6 states "Investigations and policy relating to directed surveillance and CHIS continue to be examined and discussed as part of the inspection process".

Paragraph 8.3 states "Reviewing training will continue to be a prominent part of my inspections and I expect senior officers to take a lead in ensuring that current and prospective Authorising officers are appropriately trained".

Paragraph 14.3 states "I have asked my Chief Inspector to review the OSC Inspection Strategy to optimise the inspection resources available to me and to ensure that the inspection process not only satisfies my statutory obligations but also provides a useful link to public authorities . . . It is clear that my duty of review best serves the public interest because of my statutory independence and my non-participation in policy-making".

OSC Web Site

How we work—Surveillance Commissioners

"Section 91 of the 1997 Act provides for the Prime Minister to appoint a number of Commissioners to perform certain statutory functions under Part III of the 1997 Act. These were extended in 2000 to cover oversight of Parts II and III of RIPA and RIP(S)A".

"Commissioners are responsible for . . . assisting the CSC in his duty to keep under review the use of directed surveillance and covert human intelligence sources by the law enforcement agencies".

How we work—Assistant Surveillance Commissioners

"Are responsible for:

— Assisting the CSC in his duty to keep under review the use and conduct of directed surveillance and of covert human intelligence sources (CHIS) by specified authorities.

— Examining the practices and procedures used and the records kept . . .

— Reviewing authorisations, reviews, renewals and cancellations of authorities".

How we work—Surveillance Inspectors

"The Inspectors assist the Chief Commissioner in overseeing surveillance operations carried out by the police and other public authorities".

"Inspections take the form of interviews with senior management and operational staff at all levels, assessment of documentation relating to strategies, policies and procedures and detailed analysis of individual operations".

"Assessment of corporate policies and procedures for covert surveillance:

— Written strategies, policies and procedures.

— Training policies and arrangements.

— Monitoring arrangements.

— Quality control and standard measurements and audits.

— Performance measures.

— Reviews of effectiveness of surveillance operations.

— Methods of consideration of alternative options including, for example, the level of communication with neighbouring forces and other organisations".

Inspection of individual operations include adherence to legislation and authorisation process, safeguards, knowledge levels and arrangements for storage, review and destruction of material obtained by surveillance.

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Legislation

Regulation of Investigatory Powers Act 2000 provides that:

> S57(1) "The Interception of Communications Commissioner shall keep under review the exercise and performance, by the Secretary of State of the powers and duties conferred or imposed on him by or under sections 1–11 . . . The exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II or Part

I . . . the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties conferred or imposed on him by or under Part III".

Acquisition and Disclosure of Communications Data—Codes of Practice
Oversight—

8.1 "The Act provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of part I of the Act".

8.4 "Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available to the home office to promulgate good practice and help identify training requirements within public authorities and CSPs".

8.5 "Subject to the approval of the Commissioner public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with chapter II of the Act and this code".

IOCCO Annual Report 2005–06

"To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 1 to 11 of RIPA and the adequacy of the arrangements made for the purpose of sections 15 and 16 of RIPA".

"To keep under review the exercise and performance by the Secretary of State of the powers and duties conferred or imposed by or under Chapter II of Part I (the acquisition and disclosure of communications data)".

IOCCO Web Site

There is no web site.

Her Majesty's Inspectorate of Constabulary (HMIC)

HMIC Web Site

"Her majesty's Inspectors of Constabulary are appointed by the Crown on the recommendation of the Home Secretary and report to Her Majesty's Chief Inspector of Constabulary (HMCIC), who is the Home Secretary's principal professional policing advisor. The HMCIC is independent both of the Home Office and of the Police Service".

"The inspection process is built around a series of inspection protocols which are used to examine identified functions, issues or areas of operations".

"The protocols are designed to link with each other . . . Use of the protocols will allow the examination of how far in each force the strategic leadership provides the enabling framework within which the tactical response can deliver the key objectives which attain the aims and allow successful fulfilment of the purpose".

"Each protocol has a standard structure".

Inspection Protocol: Covert Policing Methods

"This protocol sets out the questions to which Her majesty's Inspectors will require answers regarding the police use of surveillance, undercover policing, informants, and the interception of communications. It will not include detailed questions on matters subject to oversight by independent commissioners".

Areas covered in the protocol are:

> *Leadership*: "How the behaviour and actions of managers inspire, promote and support excellence in covert policing to achieve force objectives".
>
> *Policy and Strategy*: "How the force purpose is achieved through a clear strategy based on consultation and supported by policies and objectives that have clear targets".
>
> *People*: "How the full knowledge and potential of staff working in covert policing is managed and released".
>
> *Partnerships and Resources*: "How the units plan and manage their external partnerships and the use of internal resources to achieve strategic aims and objectives".
>
> *Processes*: "How senior managers and specialist units identify, manage, review and improve covert policing processes in order to deliver the policy and strategy". Within this they do examine authorities and records for surveillance, communications data and CHIS.
>
> *Results*: "What is being achieved through covert policing in relation to external and internal customers, staff, wider societal responsibilities and against planned performance".

WEDNESDAY 30 JANUARY 2008

Present	Bledisloe, V	O'Cathain, B
	Goodlad, L (Chairman)	Peston, L
	Lyell of Markyate, L	Quin, B
	Morris of Aberavon, L	Rowlands, L
	Norton of Louth, L	

Memorandum by GeneWatch UK

SUMMARY

1. England and Wales are the only countries in the world which keep DNA profiles and samples from innocent people and people convicted of minor offences for life. The National DNA Database is an important tool in criminal investigations. However, the practice of taking DNA routinely on arrest for all recordable offences and retaining both DNA samples and the computerised DNA profiles permanently, is disproportionate to the need to tackle crime.

2. The change in legislation allowing DNA records to be retained even if an individual is never charged or is acquitted has subsequently been used to justify a change in policy which means that all Police National Computer (PNC) records are now kept permanently. The retention of permanent records of arrest (for all recordable offences) is unprecedented in British history.

3. The rapid expansion of the National DNA Database has enormous implications for the balance between the power of the state to implement "biosurveillance" on an individual and the individual's right to liberty and privacy. There is also significant potential for others—including organised criminals—to infiltrate the system and abuse it, for example by using it to reveal changed identities and breach witness protection schemes.

4. The permanent retention of all DNA profiles, samples and police records, significantly changes the relationship between the individual and the State. Individuals with records on the DNA Database lose their presumed legitimacy to go about their daily life, their right to refuse to take part in genetic research and their right to keep their family relationships and other genetic information private. Even if they have never been charged or convicted of any offence, they may be refused employment or a visa as a result of the retention of a permanent record of their arrest on the PNC. The retention of an individual's DNA profile also allows their movements to be tracked or their relatives to be identified. The potential implications for the right to protest are particularly serious.

5. There has been little public or democratic oversight of this shift in approach and current safeguards are inadequate to prevent errors or abuses. Proposals to further expand police powers and to share more DNA data with other countries will exacerbate this situation.

6. It is difficult to reconcile the current situation with the principle of equal application of the law (the concept that everyone is equal before the law). Additional constitutional protection is therefore necessary to prevent excessive "biosurveillance" of this group of citizens by this or future governments.

INTRODUCTION

7. GeneWatch UK is a not-for-profit policy research group concerned with the science, ethics, policy and regulation of genetic technologies. GeneWatch believes people should have a voice in how these technologies are used: our aim is to ensure that genetics is used in the public interest.

8. Our submission is concerned with the National DNA Database (NDNAD), which is the largest in the world. Police powers to take and retain DNA have expanded rapidly in recent years and a current Home Office Consultation proposes to expand these powers further. These changes have major implications for the privacy of citizens and their relationship with the State.

Background

9. The police in England and Wales now routinely take DNA samples without consent from anyone aged ten or above in police detention who has been arrested in connection with any recordable offence. All DNA samples are kept permanently by the companies that analyse them, and the computerised DNA profiles and personal data (such as name and ethnic group) are also kept permanently on the National DNA Database (NDNAD), linked to the stored samples by a unique reference number.[1, 2] Volunteers, including victims of crime, must give their consent for their computerised DNA profiles to be entered on the National DNA Database, and the collection of DNA from children under 10 years-old requires parental consent. However, in England and Wales consent is irrevocable and cannot be withdrawn.

10. This is out of step with practice in other European countries and with the principles adopted by bodies such as the Council of Europe,[3] which require time limits on retention of DNA records for all but the most serious offenders.

11. People who have been arrested have an arrest summons number (ASN) included in their record on the NDNAD, which provides a link to other information on the Police National Computer (PNC). The change in legislation allowing DNA records to be retained has subsequently been used to justify a change in policy which means that all PNC records are now kept permanently.[4] The retention of permanent records of arrest is unprecedented in British history.

12. A recent Home Office consultation proposes further extending police powers and implies a new link between the NDNAD and the proposed National Identity Register.[5] Proposals under the Prüm Treaty may in future allow direct access to the NDNAD, or some of the information it contains, by law enforcement agencies in other European Union countries.[6]

Uses of the NDNAD

13. Every night a "speculative search" of the NDNAD is run to look for new DNA profile matches. A match between an individual's computerised DNA profile and a crime scene DNA profile indicates a high probability that the individual was at the crime scene.

14. A DNA database is not required to provide evidence of guilt or innocence when there is a known group of suspects for a specific crime. The "added value" of putting individuals on a database is only to introduce new suspects into an investigation.

15. DNA matches between crime scenes and individuals on the Database include many matches with victims and innocent passers-by. Only some matches (called DNA detections) involve sufficient evidence to charge someone for a crime, and not all DNA detections lead to prosecutions or convictions.

16. Uses of the NDNAD may include any purpose related to the prevention or detection of crime. Uses currently include: familial searching (using partial DNA matches to try to identify the relatives of a suspect); searching by name; and undertaking various types of genetic research (including controversial attempts to predict ethnic appearance from DNA).[7]

Does permanent retention of DNA samples and computer records on the NDNAD change the balance between citizen and state? What effects are there on a citizen's liberty and privacy and the character of citizenship?

17. The law allows the capture and use of genetic information without consent from a defined section of the community (those who have been arrested for a recordable offence), often referred to as the "active criminal population" (despite the fact that many of these individuals will not have committed any crime).

[1] GeneWatch UK (2005) The police National DNA Database: Balancing crime detection, human rights and privacy, GeneWatch UK, January 2005, http://www.genewatch.org/HumanGen/Publications/Reports/NationalDNADatabase.pdf

[2] GeneWatch UK(2005) The police National DNA Database: human rights and privacy, GeneWatch UK Briefing Number 31, June 2005, http://www.genewatch.org/publications/Briefs/brief31.pdf

[3] Recommendation No 92 on the use of analysis of deoxibonucleic acid (DNA) within the framework of the criminal justice system (adopted on 10 February 1992).

[4] Coates F (2006) Police to file all offences for life, *The Times*, 21 January 2006, http://www.timesonline.co.uk/section/0,,2086,00.html

[5] Modernising Police Powers: Review of the Police and Criminal Evidence Act (PACE) 1984, GeneWatch UK submission to the Home Office consultation, May 2007, http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/HO_consul07_fin.doc

[6] Johnston P, Waterfield B (2007) DNA data deal "will create Big Brother Europe", *The Telegraph*, 18 February 2007. http://www.telegraph.co.uk/news/main.jhtml;jsessionid=GAUE2T1MP0CL5QFIQM GCFGGAVCBQUIV0?xml=/news/2007/02/16/ndna16.xml

[7] GeneWatch UK(2006) Using the police National DNA Database—under adequate control? GeneWatch Briefing, June 2006, available on: www.genewatch.org

18. People on the Database are treated as members of a "risky population", whose DNA requires permanent retention by the State.[8] Young people, people suffering from mental illness and people from black and minority ethnic groups are particularly likely to be members of this "risky population". Retention of an individual's DNA profiles on a Database is likely to be of most benefit when he or she has a record as a "career criminal" and is considered likely to re-offend. However, the population on the Database now includes anyone who is arrested for a recordable offence. Ministers have accepted that: "As far as we are aware, there is no definitive data available on whether persons arrested but not proceeded against are more likely to offend than the population at large."[9]

19. DNA and fingerprints differ from other means of surveillance, such as photographs and iris scans, because they do not require equipment to be installed in particular places in order to trace or record where an individual has been. Both DNA and fingerprints may be left wherever a person goes. The retention of DNA and fingerprints from an individual on a database therefore allows a form of biological tagging or "biosurveillance".[10]

20. Unlike fingerprints, DNA can also be used to investigate biological relationships between individuals (including paternity and non-paternity). A person's DNA also contains some other private information about their health and other physical characteristics. Some of this information (such as carrier status for a genetic disorder and non-paternity) may be highly sensitive and/or unknown to the individual.

21. The routine use of "speculative searches" of the NDNAD means that any individual with a record on it may become a suspect for a crime as a result of a match between their DNA profile and a crime scene DNA profile.

22. Because a DNA match does not provide certainty that the individual committed the crime (many DNA matches are with the DNA of passers-by, and a few occur by chance), this process entails a subtle shift in the burden of proof and the presumed legitimacy of people on the Database to go about their daily lives. New techniques may also make false matches more likely. For example, the increasing use of Low Copy Number (LCN) DNA analysis—which allows a DNA profile to be extracted from a single cell—has led the Director of the Forensic Institute in Edinburgh to warn that innocent people may be wrongly identified as suspects as a consequence of being on the NDNAD[11] and the judge in the Omagh trial to criticise specialist evidence on this technique as contradictory.[12] In one case this technique reportedly identified a 14-year old English schoolboy as a suspect for having planted a Real IRA car bomb.[13] The use of "familial searching" means that anyone who is genetically related to an individual on the Database may also become implicated as a suspect.[14]

23. Because an individual may leave DNA wherever they go, there is also potential for it to be used to try to identify whether he or she has been present at scenes other than crime scenes (for example, a political or religious meeting). The legal restriction of uses to "purposes related to the prevention and detection of crime" provides no meaningful barrier to such surveillance, nor is there any independent scrutiny which could identify such uses. Particular concern arises in the context of the right to protest, because acquittal by a court, or a spent conviction for a relatively minor offence, no longer results in removal of a person's record from the NDNAD or the PNC.

24. Allowing the Database to be searched by name, or by using a "familial search" (looking for partial matches between a DNA profile and profiles stored on the Database), means that an individual's DNA profile can be obtained and used to trace their movements or identify relatives. If a person's DNA sample is also accessed, other personal genetic information may also be obtained. The same approach may be used to trace identifiable groups of individuals (for example, searches for the DNA profiles of people belonging to a particular ethnic group or having "typical Muslim names" have been made in the context of research projects undertaken using the NDNAD).

25. The permanent retention of an individual's record of arrest (including the retention of their record on the PNC, linked to the NDNAD) may also be used to deny them access to employment or visas, or restrict their rights in other ways (for example, they lose their right to refuse to take part in controversial genetic research). Even after records are "stepped down" on the PNC (so that access by agencies other than the police is supposedly restricted) information contained in these records may continue to be made available to others as

[8] McCartney C (2004) Forensic DNA sampling and the England and Wales National DNA Database: a sceptical approach, Critical Criminology, 12, 157–178.
[9] *House of Commons Hansard* 9 October 2006: Column 491W.
[10] Williams R, Johnson P (2004) Circuits of surveillance, Surveillance and Society, 2(1), 1–14.
[11] Morgan J (2006) Guilty by a handshake? *The Herald*, 2 May 2006.
[12] Fresh criticism of Omagh evidence, BBC Online, 8 December 2006. http://news.bbc.co.uk/1/hi/northern_ireland/6162483.stm
[13] McCaffrey B (2006) Controversial DNA tests identified schoolboy as part of Omagh attack, *The Sunday Business Post*, 12 November 2006. http://archives.tcm.ie/businesspost/2006/11/12/story18791.asp
[14] Williams R, Johnson P (2005) Inclusiveness, effectiveness and intrusiveness: issues in the developing uses of DNA profiling in support of criminal investigations, *Journal of Law and Medical Ethics*, 33(3), 545–558.

the result of an Enhanced Criminal Record Check.[15] Employers may also require an individual undertake his or her own subject access request to the police and reveal this as a condition of employment (known as "enforced subject access").

26. The rapid expansion of the National DNA Database therefore has enormous implications for the balance between the power of the state to implement "biosurveillance" on an individual and the individual's rights to liberty and privacy.

Is the Data Protection Act sufficient in safeguarding constitutional rights?

27. The Data Protection Act is inadequate in principle because it does not restrict the retention or use of individuals' DNA samples or computer records in any meaningful way: it does not prevent State "biosurveillance" of any individual with a record on the Database.

28. The Act is also inadequate in practice because its focus is on control of access to the Database itself. In practice, the process of collecting, analysing and storing DNA allows numerous points of access to confidential information (for example, by employees working in the commercial laboratories which analyse and store the DNA samples for the police; or by the non-police staff who may collect DNA in the proposed new Short-Term Holding Facilities). If criminals can infiltrate the system they may be able to use it to identify people whose identity is protected, including people in witness protection schemes and undercover police officers, and to trace their relatives or reveal private genetic information (including paternity and non-paternity). The risk to privacy is also increased by plans to share more information with EU countries and to check DNA or police records on the spot using hand-held devices.[16, 17]

29. There have already been a number of incidents and practices which cause serious concern:

- Five employees of the Forensic Science Service (FSS) have been suspended whilst allegations that they "copied, retained and/or adapted software and/or other confidential information" are investigated.[18]
- Emails supplied to GeneWatch UK as a result of a Freedom of Information request revealed that the commercial company LGC kept copies of information sent to it by the police, including individuals' demographic details, alongside their DNA profiles and samples.[19, 20]

Do the benefits outweigh the concerns? Where should the line be drawn?

30. The practice of retaining individuals' DNA samples and computerised DNA profiles permanently is clearly disproportionate to the need to tackle crime.

31. The value of entering increasing numbers of DNA profiles from individuals on the Database (unrelated to the reason for arrest) is that it may allow investigation of a past crime to be re-opened, by unexpectedly identifying a new suspect. The purpose of retaining an individual's DNA profile on a database is to treat them as a suspect for any future crime.

32. Re-examination of a number of "cold" cases has highlighted the importance of keeping past crime scene DNA evidence. Occasionally, the DNA of someone arrested for a minor offence is matched with DNA from a serious past crime, arguably justifying taking DNA from relatively large numbers of individuals. Examples of such cases have been provided to Parliament and to the public in an attempt to justify expansion of the Database.[21, 22] However, such cases do not justify permanently retaining DNA profiles and samples from people whose DNA has not matched a past crime scene.

33. Analysis of Home Office data shows that collecting more DNA from crime scenes has made a significant difference to the number of crimes solved, but keeping DNA from increasing numbers of individuals has not.[23] Since April 2003, about 1.5 million extra people have been added to the Database, but the chances of

[15] ACPO (2006) Retention guidelines for nominal records on the Police National Computer, 16 March 2006.
[16] Adams L (2006) Police computer goes on the beat, *The Herald*, 14 October 2006, http://www.theherald.co.uk/news/72189.html
[17] For example: http://www.itweek.co.uk/vnunet/news/2170113/portable-dna-analyzer-invented.
[18] Gallagher I, Myall S (2007) Five civil servants suspended over "DNA espionage", *Mail on Sunday*, 31 March 2007. http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=445902&in_page_id=1766&in_a_source=&ito=1490
[19] http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/AnswerFOI8May.pdf
[20] Barnett A (2006) Police DNA database is "spiraling out of control", *The Observer*, 16 July 2006, http://observer.guardian.co.uk/uk_news/story/0,,1821676,00.html
[21] *House of Lords Hansard* 26 April 2007 : Column WA152.
[22] The National DNA Database Annual Report 2005–06, www.homeoffice.gov.uk/documents/DNA-report2005-06.pdf
[23] GeneWatch UK (2006) The DNA expansion programme: reporting real achievement? February 2006, http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAexpansion_brief_final.pdf

detecting a crime using DNA has remained roughly constant, at about 0.36%.[24] The Home Office appears to accept that the retention of DNA from innocent people has had little impact on crime detection rates[25] and seems unable to quantify the claimed benefits.[26] In Parliament, ministers have repeatedly provided figures for DNA matches, rather than detections or convictions. DNA matches are much more frequent than successful prosecutions—they will include many matches with the DNA of victims and of passers-by. Despite the lack of evidence on successful prosecutions, the figures on matches have repeatedly been used by ministers to justify the changes in the law[27] and have also frequently been misreported as "solved" crimes.[28]

34. Retention of individuals' DNA samples increases privacy concerns and costs (the companies which store them are paid an annual fee). Individuals' samples are destroyed in some other countries, such as Germany, once the computerised DNA profiles used for identification purposes have been obtained. The Home Office has recognised that retaining samples is "one of the most sensitive issues to the wider public"[29] and the Human Genetics Commission has concluded that the reasons given for retaining them are "not compelling".[30, 31] Only temporary, not permanent, storage is necessary for quality assurance purposes and a new sample can always be taken from the suspect if a DNA profile requires checking or upgrading.

35. GeneWatch UK believes that there are important changes that could be made that would improve safeguards for human rights and privacy without compromising the role of the DNA Database in tackling crime. A better balance would be struck by:

- reintroducing a system of time limits on how long people are kept on the Database—so that only DNA profiles from people convicted of serious violent or sexual offences are kept permanently;
- destroying all individuals' DNA samples once an investigation is complete, after the DNA profiles used for identification have been obtained;
- ending the practice of allowing genetic research using the Database or samples, so that research is limited to performance management and database improvements;
- better governance, including an independent regulator;
- public and parliamentary debate before new uses of the Database are introduced;
- a return to taking DNA on charge rather than arrest, except where it is needed to investigate a specific offence.

Is there a need for any additional constitutional protection of citizens?

36. The permanent retention of DNA profiles and samples from large numbers of individuals who have committed no offence, or have a spent conviction for a minor offence, significantly changes the relationship between the individual and the State.

37. Individuals with records on the National DNA Database are treated as a "risky population", whose DNA requires permanent retention by the State. They lose their presumed legitimacy to go about their daily life, their right to refuse to take part in genetic research and their right to keep their family relationships and other genetic information private. Even if they have never been charged or convicted of any offence, they may be refused employment or a visa as a result of the retention of a permanent record of their arrest on the PNC. The retention of an individual's DNA profile also allows their movements to be tracked or their relatives to be identified.

38. It is difficult to reconcile this situation with the principle of equal application of the law (the concept that everyone is equal before the law). Additional constitutional protection is therefore necessary to prevent excessive "biosurveillance" of this group of citizens by this or future governments.

1 June 2007

[24] GeneWatch UK (2007) The National DNA Database: an update. Human Genetics Parliamentary Briefing No 7, January 2007, http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/MPs_Brief07.pdf

[25] Burnham A (2006) Letter to GeneWatch, 15 March 2006.

[26] *Hansard* 1 February 2006: Column 569W, http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm060201/text/60201w25.htm#60201w25.html_sbhd3

[27] Under−18s DNA records to continue, BBC Online, 16 February 2006, http://news.bbc.co.uk/1/hi/uk_politics/4720328.stm

[28] DNA solves 500 offences, *The Sun*, Friday 17 February, http://www.thesun.co.uk/article/0,,2-2006070843,00.html

[29] Home Office (2005), Supplementary Memorandum, Appendix 20. In: House of Commons Science and Technology Committee (2005) *Forensic science on trial*, Volume II. HC 96-II, www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96ii.pdf

[30] Human Genetics Commission (2002). Inside information, May 2002, http://www.hgc.gov.uk/UploadDocs/DocPub/Document/insideinformation_summary.pdf

[31] Human Genetics Commission (2005) HGC response to the Scottish Executive consultation on police retention of prints and samples. http://www.scotland.gov.uk/Resource/Doc/77843/0018244.pdf

Examination of Witnesses

Witnesses: PROFESSOR PETER HUTTON, Chairman, National DNA Database Ethics Group, PROFESSOR GRAEME LAURIE, University of Edinburgh, and DR HELEN WALLACE, Director, GeneWatch UK, examined.

Q154 ***Chairman:*** Could I welcome you, Professor Hutton, Professor Laurie and Dr Wallace. It is extremely good of you to come and give evidence. We are not being televised but we are being recorded, so I would ask you, if I may, to state your names and organisations for the record, and thereafter to make a short opening statement if you so wish.
Professor Hutton: My name is Professor Peter Hutton; I am here as the Chairman of the National DNA Ethics Group, which was set up as a non-departmental public body on 25 July last year. My full time employment is as a Professor of Anaesthesia and Honorary Consultant at the University Hospital, Birmingham, and Birmingham Medical School.
Professor Laurie: Good morning; I am Professor Graeme Laurie from the University of Edinburgh Law School. I am also here as a representative of the Nuffield Council on Bioethics. I was recently a member of the Working Group on ethical issues related to bioinformation, and the terms of reference of that Council are to identify and define ethical questions raised in respect of biomedicine and bioethics and to report publicly on those issues.
Dr Wallace: My name is Dr Helen Wallace. I am the Director of GeneWatch UK, which is a small, not for profit organisation set up about ten years ago. Our aim is to ensure that genetics is used in the public interest and to stimulate public debate about the applications of genetic technology.

Q155 ***Chairman:*** Would anybody like to make a brief opening statement or shall we go straight to questioning?
Professor Hutton: I am happy to go to the questions.

Q156 ***Chairman:*** Could I ask, to begin with, if you could give us a brief explanation of the nature of DNA samples and profiles and how they are collected? And to what extent is the technology advancing?
Professor Hutton: The DNA which is present in almost every cell of our body is identical on every occasion, although its activity differs from cell to cell. Of the DNA which is present in the cell only five per cent of that DNA is actually used to make body cells and components; the remaining 95 per cent of the DNA is what is termed scientifically as redundant DNA, that is, it has no known purpose in producing the cells of the body. It has other purposes about which people speculate, such as providing structural integrity to the molecule. When a forensic DNA test is done it is the redundant part of the DNA which is tested, not the section which is responsible for the production of cells. When we are conceived, we inherit 50 per cent of our DNA from our mother and 50 per cent from our father. The gene which, for instance, produces a normal compound such as insulin is probably the same in each parent. However, the redundant components of DNA differ greatly from person to person and that it is why it is that section which is used to differentiate identity. The tests which are done are done by applying substances called primers which stick to particular components of the DNA. Depending upon where they stick and the amount that they stick to determines your DNA profile, and that emerges either on a paper printout or on an electronic screen as a series of numbers and peaks, and for any one individual 50 per cent of those numbers and peaks will be determined by their mother and 50 per cent by their father. That is also true of a sibling but it is a different 50 per cent from each parent. In that way siblings are similar but inherently different to each other. The tests which are used in Britain are based on a system called SGM Plus, which stands for Second Generation Multiplex—that is the name of the machine—and Plus because it is a more advanced test. This tests the redundant DNA at ten positions and also identifies the sex chromosomes, and, in comparing DNA if you test the ten positions together with the sex chromosome the chance of a match at random is one in a billion. I think perhaps, my Lord, if I stop there people could ask questions.

Q157 ***Chairman:*** Thank you very much indeed. Could I ask what estimate you would make about the reliability of DNA samples and profiles in the context of law enforcement?
Dr Wallace: Perhaps I could answer that? I think it is clearly highly reliable; if you have a complete DNA profile from the individual and a complete DNA profile from the crime scene the match probability is roughly one in a billion.

Q158 ***Chairman:*** Could you say that again?
Dr Wallace: The probability of a match with an unrelated individual, if you have two full profiles, is around about one in a billion. However, there are quite a number of steps along the process where problems can arise. First, you will notice that I said an unrelated individual—there is of course a potential that relatives become the subject of an investigation and may be wrongly implicated. Secondly, there is a big issue about crime scene DNA but the crime scene itself is obviously a messy place to collect DNA samples and many of those samples do not give a complete DNA profile. So, for example, in 2005/2006 something like 50,000 of the match reports sent to the police involved a list of potential suspects and that was largely due to the fact that the crime

scene DNA profiles were not complete. So it is a misunderstanding to think that a single individual is often implicated in the crime. The second point to emphasise also is that at a crime scene many people may have been present who are not necessarily the perpetrators, so you may also have a match with someone who has been at the crime scene earlier in the day, for example.

Professor Laurie: May I just add that one of the significant technological developments that struck the Working Group was the ability to obtain DNA from smaller and smaller samples, known colloquially as low copy number, and this has been heavily criticised in the recent Omagh bombing trial and is currently being investigated by Sir Brian Caddy at the request of the interim Forensic Regulator. One of the concerns is the lack of scientific and international agreement about the reliability of this in terms of what it can actually say for matches in criminal trials and we understand that it has been reported that only three countries routinely rely on this sort of evidence—the United Kingdom, the Netherlands and New Zealand. Such a review was welcomed by the group because one of the main concerns of the Working Group was public trust and confidence in the quality of the forensic service provision.

Q159 ***Baroness Quin:*** In the account of the ethical issues of the organisation in which you are involved it does say in paragraph three that in particular there are dangers of deliberate or accidental contamination, misinterpretation of mixed samples and mistaken interpretation of the partial profile. Are there examples that you know of where this has happened and where injustice has resulted?

Professor Laurie: It is important to understand the context in which the report was actually drafted. It was not really the business of the Council to try and look for case studies; it was more to reassess the fundamental ethical principles upon which our entire system is actually based. A lot has to go wrong before there are actual specific incidences of miscarriages of justice but what comes out of our report is that the ethical principles we feel should inform the entire process are those of liberty, privacy and autonomy and there can be many intrusions on an individual's privacy before they actually get to court and before that may lead to problems of miscarriage, and it was really about getting the balance right between what is in the interests of society and the prosecution and detection of crime and citizens' interests of privacy and liberty.

Q160 ***Baroness Quin:*** None the less, have there been any examples as far as you know of, say, a contamination?

Professor Laurie: There are examples of contamination, absolutely, and there is also an interesting example that comes up in respect of people who wish to be removed from the database and having problems in achieving that because the system as it is currently set up is actually difficult to penetrate and the system does not necessarily pay due respect to the concerns that people have for privacy and liberty that underpin everything.

Q161 ***Baroness O'Cathain:*** This is getting away from the particular to the general, but in your introduction somebody said the report to the "interim Forensic Regulator" so does that mean that there is not actually a person in post who is in charge of forensic regulation and is that a problem?

Professor Hutton: The Home Office decided that there should be a Forensic Regulator. The interim Forensic Regulator is one of the Home Office officers called Adrian Cory. He set up the Regulator's office and in fact demits office as the interim Regulator at the end of this month and will be replaced by a full time Regulator, Andrew Rennison.

Q162 ***Lord Morris of Aberavon:*** Could I come back, Lord Chairman, to the state of the art and liability? When I prosecuted and defended, in latter years with the development of DNA one assumed that DNA was always infallible and you could not challenge it. In view of the recent observations at the Omagh trial does that still stand? And is this a developing art since Doctors Crick and Watson made their great breakthrough? Has it developed?

Professor Hutton: Could I answer that, my Lord? I think if one looks first of all at the analysis process of DNA written into the contractual relationship between the laboratory and the police service there are parts which determine the quality assurance of the actual process itself—that is, the actual analysis of the DNA itself from a sample. I think that these are reasonably thorough and the checks and balances at this stage make it extremely unlikely that there will be an error analysis in a full DNA sample as the system is at the moment. The problems arise because the samples which are obtained from crime scenes are not always complete; they are there because they have been left there for a variety reasons. DNA is an extremely stable molecule (it clearly has to be like that because it has to keep us going for 70 plus years) but despite that it can be broken down by various environmental factors such as chemicals and heat. In addition, when a sample is taken at the crime scene it may not be possible to get a full strand of DNA. This means that the analysis on the crime scene samples is frequently on an incomplete sample and so the whole spectrum of a DNA profile will not be revealed by the laboratory but just part of it, and it is this part of the sample which is then compared with the people on

the National DNA Database or other suspects. As a result of that there are more suspects revealed because the number of components you are comparing is less than there optimally would be. In relation to the question has it ever resulted in a miscarriage of justice, as far as I know in the English system nobody has been prosecuted on the evidence of DNA alone; there has had to be corroborative evidence related to the actual crime. So in essence, it leads the investigative services to suspects, it does not alone, as I understand it to date in England, produce a conviction. There is a further complexity—and I mention it now in case it gets asked—to do with cold cases, which are cases that are reviewed by the police now that have occurred some time in the past. The whole basis of cold case analysis is that samples from that crime scene—clothing, office bits and pieces, that sort of thing—are re-examined for DNA. Using more modern techniques you can extract the DNA from the smaller sample, and this is what has subsequently led to reopening of investigations and the successful prosecution of people, not on the DNA *per se* but the DNA has led them to the person who has subsequently been charged and convicted.

Q163 ***Lord Morris of Aberavon:*** How damning is the fact that you only get from a scene of crime a partial sample? We have always had that with fingerprints—you needed 16 characteristics and as you go down the line you become less confident. Is there a yardstick of completeness that you can put before the jury so that they can reach a conclusion beyond reasonable doubt?

Professor Hutton: If I could offer an opinion but not as an expert because I do not work in a DNA laboratory? If you are looking, say, at paternity testing where you have three good samples—one from the putative mother, one from the putative father and one from the generated individual then, as it were, the overlay with the samples will be exact and can be done by computer reading. If however you are looking at a situation in which the crime scene sample is deficient—and in many ways it may be corrupted—then there enters a component of judgment on the basis of the laboratory technician who is looking to make the comparison. There are, as I understand it, computer programmes to assist with the exclusion of people who could not possibly be matched, but when it comes down to the actual comparison of a low copy number with the full profile of the suspect then judgment is involved. Again, it is my understanding that because of that, low copy number and boost techniques, which are techniques to produce more replicated DNA from what is available, are only used as supportive examination. I do not know the details of the Omagh trial but my understanding informally is that there was going to be a bias towards giving greater weighting to the DNA evidence on that occasion.

Q164 ***Lord Lyell of Markyate:*** If I may briefly ask two questions. The more we can learn about the Omagh trial will be helpful because the prosecution obviously believed in the DNA evidence or they would not have put it forward, and it seems to have been an alert judge and good cross-examination which brought the faults to light. But with DNA in criminal trials you get manipulators, you get people who are planning trials and may want to make it seem as though it is somebody else, so how easy would it be for them, by leaving a piece of clothing or something around or in some more subtle way, to cause the DNA evidence to be corrupted?

Dr Wallace: Perhaps I can say something because I think there are a number of different issues involved here. For the low copy number technique, for example, the judge, I think, particularly focused on the reliability of the laboratory process used to extract that DNA profile from a single cell and that is what is currently being investigated. But there is also another issue about contamination that relates to your follow-up question. So one concern that has been raised is that because it is based on a single cell, that DNA could have been transferred to the crime scene not directly by the individual involved. So, for example, if I shook hands with you and then went on to commit a murder a single cell of your DNA might end up on the murder weapon, without you necessarily having been there. So there are a number of different factors. There is also another technique called DNA boost that has just been introduced and that is about separating DNA profiles statistically from mixed DNA samples, which again may solve more crimes but may also introduce new errors. I want to come back to the point that Graeme made, that there are two issues here; there is an issue about whether people get implicated in investigations, whether or not there is a subsequent miscarriage of justice, because when we talk about the DNA database if you are aware that the majority of matches do not lead to a successful prosecution. Then, when you consider the privacy issues you have to be aware that you may be implicated in an investigation that may of itself be problematic for that individual, without necessarily there being a miscarriage of justice. In relation to miscarriages of justice I think the simple answer is that nobody knows; how would you know, frankly, if somebody had been falsely convicted?

Q165 ***Viscount Bledisloe:*** Can I first of all pick up on a point that Dr Wallace made? All sorts of things lead to people being implicated in an investigation but they are not eliminated, and that is inevitable, is it not?

Dr Wallace: It is inevitable but I think there is a difference between the type of investigation that I would say perhaps we could call it an Agatha Christie scenario, where there is a limited number of people who may be implicated in a crime that have their DNA tested, who are the subject of that investigation, and a situation where potentially millions of people, however many people are on the database, may be implicated through a match on that database. We are moving then into a situation which I think comes up more in your further questions—what are the downsides in relation to that?

Q166 ***Viscount Bledisloe:*** The other thing I want to take up is that you said nobody had been convicted on DNA evidence alone and there has to be some corroborating evidence, but there must be lots of cases, must there not, where although there is some other evidence without the DNA evidence they probably would not have been convicted?
Professor Hutton: I am answering this not as a legal person but just from my understanding of the situation. My understanding of the situation is that the majority—and actually as far as I know all, the convictions that have occurred involving DNA have been ones in which the DNA has led the investigators to a number of suspects, but it is other evidence which has convicted the individual. That is my understanding.

Q167 ***Lord Peston:*** I am terribly bewildered by all of this, I must say. The second question has been largely answered, but we seem to be—and I include the witnesses in this—totally confused between the natural science and what you might call social science. The fact is that my DNA is my DNA, a natural scientific phenomenon. I am certainly not qualified in that area but I know enough to know that my DNA is my DNA. That is quite different from raising the points that are being raised—which I am totally unsympathetic to, I might say, but that is not your problem—that we can misuse. But we know that anything in the scientific area can be misused, to which I ask you "so what" especially given the evidence we have heard that court cases still take place as proper court cases? Even if you are there and say, "I saw him shoot the gun" the other side will still argue with you and say, "Are you sure you saw him? Were your glasses on properly?" and so on. So I do not quite see what this song and dance is about special ethical issues concerning DNA; it is totally beyond me, and I am certain that the great inventors of genetics would be amazed at your response to one of the greatest discoveries in the history of science. I put it to you, what is it that is really troubling you, other than the fact that we are all human and we make mistakes, but that is why we have a legal system?
Professor Laurie: The thinking behind the Nuffield Council Bioethics Working Group was that actually this was a very opportune time to look at the ethical issues because there are concerns about the extent to which, in Britain particularly, the DNA database was expanding, the extent to which uses may be made of that database, which were not legitimate and were not justified. Yes, you are absolutely correct we have a legal system but the legal system which we have is one which is framed by human rights, and those human rights reflect certain civil liberties and fundamental values such as liberty, privacy and respect for autonomy, and are in terms of the sort of society in which you want to live; if then we have something that is potentially powerful and useful as this National DNA Database and if it is being misused it may actually not only go against the interests of individuals who may suffer miscarriages of justice but it may go against the interests of all of us if the fundamental social objective of prosecuting crimes is not actually achieved. So what we were trying to do with this report was to look at the ethical issues and to say that there is an awful lot of value which comes from looking at that natural material and using that to detect and prosecute offenders, but at the same time to ask do we have sufficient measures to safeguard the liberty and privacy of people who are innocent who may also be implicated? That was the balance that we were trying to look for.

Q168 ***Baroness Quin:*** I am not sure that my good colleague Lord Peston will approve of these questions because I think they do relate to the proportionality and threats to the individual issues. Can I ask in terms of the use and collection of DNA information to what extent do our witnesses feel that retention gives rise to treating people as suspects for future crimes?
Dr Wallace: We think there is quite a clear distinction between collection and use of DNA and its retention. So clearly it is an extremely valuable tool, I would certainly agree with Lord Peston in terms of the investigation of a specific crime. The questions arise when the DNA is used more broadly by adding it to a database or adding the computerised DNA profile to the database. There are two purposes essentially to that. The first purpose, which is routinely used when that profile is added, is to look for matches with any past crime scene profiles, which is something that clearly can implicate somebody in a past crime scene. The second use is retaining that data to look for matches with any potential future crime scene profile, and this is where we feel that particular new ethical issues arise because retention in effect is a kind of biological tagging—it is a form of keeping somebody on the database just in case they commit that future crime and it has, therefore, some downsides in terms of the potential threat to genetic privacy if the

samples themselves are revisited, which are also stored. It also creates a permanent list of suspects if those records are linked to a permanent record of arrest and are kept on the Police National Computer with access by various agencies. And it creates the potential for abuse either by governments in terms of surveillance or by anyone who might infiltrate the system. So I think there is quite a range of issues there.

Professor Hutton: If I could just fuse the two questions, the one from Lord Peston and this one? I think that there is a problem in the law in that the UK Human Tissue Act actually states that your DNA is part of your body and for a non-consensual test you have complete rights over what happens to it. That is one problem. The manner in which consent is taken from people who are volunteering their DNA is a key question and it is being looked at by the Ethics committee which I chair. I think that is an issue. The second point is that there is a huge difference between the DNA profile and the actual DNA sample itself. The DNA profile at the current state of science can only really be used for inheritance testing or relationship establishment. In addition, and I do not want to say whether this is good or bad—an extra sample is retained by the police of the entire DNA, which includes not just the redundant DNA but it also includes the DNA which codes for protein. It is that component of DNA that would be the predictor in some instances of disease, of life expectancy and of a number of issues which might affect your relationship with the insurance industry. One of the worries of members of the public is that if the DNA sample *in toto* is retained that it could be misused for a purpose for which it was not intended. That is actually part of the reason why the law—I think it was in 2003, I have the reference—was made such that it was specific that the DNA, if was collected for a judicial purpose could only be used for the purposes of the prosecution of crime. That principle has been tested by people requesting DNA on the National DNA Database to be used in paternity testing and the request has been rejected. The only exception to that was an amendment to an act in 2005 which allowed for DNA testing for people who had been killed in natural disasters, and it was the tsunami that created that amendment to the legislation. So I think what the worry of many people is, is that the retention of the second sample, which has not yet been analysed, would allow information personal to themselves to be extracted from it, if it were used for another non-intended purpose. In relation to your question, I think that public opinion was tested and reflected by the Human Genetics Commission in the submitting evidence during formation of the Human Tissue Act. In clause 45 of that it specifically states that your DNA belongs to you, to nobody else, and that includes any information derived from it unless the DNA has been taken for an accepted purpose. An accepted purpose is a custodial sample which can be taken from anybody who is arrested or detained in a police station for a recordable offence.

Q169 ***Baroness O'Cathain:*** This is really very, very significant because there is a big movement at the moment in that people will say why do we not just collect DNA from the whole population? So I take it that the three of you would be dead against that? You probably know that the Human Fertilisation and Embryology Bill has been going through our House and there have been several references to the Human Tissue Act and quite a body of opinion is actually saying that perhaps we ought to have another look at that because of all the developments in embryology and in stem cells and so on, since both Acts became law. The HFE Bill that we are dealing with at the moment is directly related to the 1990 Act. So I think this is a hand grenade with the pin hanging out if on the one hand you have people saying, "Let us do it in cases of social justice"—and we will come on to another question which makes that obvious as well—and on the other hand you are saying that it is ours and really there should be no Act. So I take it that you think we should stick with the situation that we have at the moment?

Professor Hutton: We have considered that in the Ethics Group—and I can give you a set of minutes afterwards if you wanted to refer to them—and we have taken evidence from a number of special interest groups, one of which is the Nuffield Council and another is GeneWatch, but there are others as well. If I could read out the two bullet points, just two sentences, Chairman, on our view on this, which in fact was placed on the Home Office website yesterday, so it is up to date. Is, "the reasons for taking and retaining DNA samples and profiles have never been defined in legislation. This situation has not been modified. The spirit of the original law in 1994 was not that it should become a database containing the details of the whole population. Until the change in legislation in 2001 any DNA profile sample or information derived from a custodial or volunteer sample had to be destroyed if there was no charge or conviction." And this is the key point, I think: "Although there are arguments that can be made for the establishment of a national civilian non-criminal DNA database those arguments are very different from those used for the establishment of a criminally related database. Consequently, it is our view that it is inappropriate and fraught with ethical and social problems to allow one to metamorphose into the other. Arguing that the database should be expanded to include all the population, the majority of whom will never commit a crime, just to prevent inequality and discrimination, is, on balance,

unsustainable when issues of proportionality and personal privacy are taken into account."

Professor Laurie: Can I begin by completely agreeing with Professor Hutton on this point and his last point that we have to consider issues of medical research and fertilisation, etcetera, quite separately from the issues that are being considered today. However, section 45 of the Human Tissue Act is actually about non-consensual analysis of DNA; it does not give people a property right in their body, their DNA; that is not how it is framed, it is about trying to respect individual autonomy. But within the rights framework that we have in the UK we do not talk about absolute rights, we talk about rights that can have exceptions, and the question then is to ask in the appropriate context which rights do we have and which exceptions might actually apply. So the framework that outlined the report from the Nuffield Council, for example, in the context of the National DNA Database was the fact that we have fundamental rights of liberty, privacy and autonomy and that is our starting point. If we wish to move from that then the obligation and the onus is on the state to show that it is necessary and proportionate in particular circumstances, and the circumstances obviously depend on what are the social ends that you are trying to achieve and those are very different in the criminal context compared to fertilisation or other uses of genetic material. The concerns of the Council in that sense were that the way in which we approach the regulation at the moment does not strike an appropriate balance between the fundamental rights in play and the onus that is on the state to justify: for example, indefinite retention of samples and profiles merely on arrest; for example, the removal from the database only in exceptional circumstances and at police discretion; or, finally, where there has been a suggestion of a universal database we are not convinced that that is necessary or proportionate to achieve the social ends of prosecution and detection of crime.

Q170 ***Lord Rowlands:*** Professor Hutton, do I draw this conclusion from your earlier answer, that the law as it stands is robust enough to prevent the transfer of information to insurers? Is the law as it stands robust enough to prevent that type of leaking of information or transfer of information?

Professor Hutton: Dr Wallace would like to come in on this as well. My understanding is that it is absolutely specific at the moment. The worry is—and I do not want to be too speculative—that that could potentially change in the future.

Q171 ***Lord Rowlands:*** That the law could change or the behaviour?

Professor Hutton: I am merely reflecting the concerns that people have expressed. One concern is that the law could change in the future. The second is—and this is in some ways fanciful but it has been said—that the storage of the DNA samples occurs in a variety of depots around the country and if somebody had the barcode connection between an individual and the storage code it would be possible for somebody to steal somebody's DNA. That is a worry. So the security of the depot is paramount in the minds of some people who are concerned about that.

Dr Wallace: Could I add something? I think firstly it is important for people to realise that the law is actually drawn rather more broadly than Professor Hutton suggested, in that the restriction on uses is to purposes related to the prevention or detection of crime. So it is not restricted simply to the investigation of an offence. Secondly, there are issues about the monitoring and implementation of that law. So we made a series of freedom of information requests in 2006 and we discovered a large number of research uses, for example, including going back to reanalyse samples to try to predict ethnicity on the grounds that that was a purpose related to the prevention or detection of crime, to develop techniques, to predict the potential ethnicity of an offender. Secondly, we found that the demographic details that the police collect along with the samples were being sent to the laboratories with those samples and that one of the commercial providers had, in effect, a mini database of those details and the samples. So that means that certainly the law does make it unlawful for that information to be handed to insurers, for example, but there is clear potential for infiltration or mistakes or uses that people would not consent to in terms of research on their samples.

Q172 ***Baroness Quin:*** I wanted to follow up something that I was asking about earlier, which perhaps I ought to understand but I do not think I do. If people have volunteered a DNA sample and they have not requested for their DNA information to be removed from the system is their DNA profile then retained and routinely trawled through in terms of trying to find out who committed crimes? And are the people who volunteer their DNA therefore given that information, that they will be routinely trawled through forever and ever, unless they change their minds; are they given that information in a proper way, in your view, at the time?

Professor Hutton: This is something which we looked at in the Ethics Group. We found the situation to be, shall we say, suboptimal? Could I just preface this by saying that our work on this has been completely supported by ACPO, the Association of Chief Police Officers? They recognise that there are problems. The method of taking consent is probably on occasions flawed in that the person taking consent from an

individual may not meet the basic criteria in common law to be able to answer specific questions about what is going to happen to the sample and the processes it will go through. When consent is taken from a volunteer—and volunteers come in a variety of styles, there are people who are volunteers to try and exclude them as contaminants from a crime scene, there are other people who volunteer because they want to be excluded as a suspect, so there are a variety of volunteers—the current consent form in fact has on it two options. One is to sign so that the DNA and its derived data will only be used for that case; the second is to sign to say that it can be used for that case and the second sample retained and the DNA profile loaded on to the National Database. Once it is loaded on to the National Database then it is there for 100 years and it is very difficult to get off; and removal is subject to the individual decisions of local Chief Constables. We have with ACPO undertaken a piece of work which is not yet in the public domain but will be shortly, which has demonstrated that if, in the main, for the majority of cases volunteer samples were not loaded on to the National Database and were used only for the case in hand there would be no loss to operational policing. It is one of our recommendations in the papers that have just gone on to the Web that the presumption for a volunteer sample should change from a presumption that it should be loaded on to the National Database to one in which it should just be used for the case in hand. So there is movement on that and, again, I feel I have to say that although it may be unpopular in certain parts of the judicial system the Association of Chief Police Officers understands the problem and is to date supportive of change.

Q173 ***Viscount Bledisloe:*** Can you give me two further answers on that? First of all, what proportion of the data on the National Database is derived from genuine volunteers?
Professor Hutton: As I understand it, it is a half of one per cent.

Q174 ***Viscount Bledisloe:*** As small as that?
Professor Hutton: As I understand it. I may be wrong but—

Q175 ***Lord Morris of Aberavon:*** Could we have that again?
Professor Hutton: I understand it is a half of one per cent, the actual true volunteer data that is on the database.

Q176 ***Viscount Bledisloe:*** That, I confess, surprises me, I would have thought there were a lot of volunteers because if somebody is murdered in my house or something I am obviously going to be delighted to give my DNA then and there either because I want the real villain caught or because I am frightened that if I refuse it the finger of suspicion will point against me. I would have thought it was much higher than that.
Professor Hutton: That is correct, my Lord, but not all volunteer samples are loaded on to the database.

Q177 ***Viscount Bledisloe:*** Even if some people tick the first box?
Professor Hutton: And even if some people sign the other sections, as I understand it. Not every sample is loaded.

Q178 ***Viscount Bledisloe:*** Would it not be better once the investigation is over if people were then asked can it be retained because in the trauma of the moment when the thing has happened I would have thought anyone would tick any box the policemen asked them to, whereas afterwards you may want to say, "No, now that it is cleared and everyone knows I did not do it and you have the villain, please destroy it."
Professor Hutton: That is a possible approach to it.
Professor Laurie: May I interrupt to try to answer that? I think that may be a possible approach on certain conditions: first of all that it is demonstrated that that would actually further the ends of prosecution services to have volunteers who are effectively innocent persons by retaining that information. Secondly, that it would respect the fundamental tenets of the law of consent, being informed consent, that you were fully informed—going back to Lady Quin's question—of what were the consequences of you being kept on this if it is indefinitely. Thirdly, hopefully it is not "indefinitely" because your right to refuse, again a fundamental tenet of the law of consent, should be respected, whereas at the moment it is not.
Professor Hutton: I have the data here; should I read it out, Lord Chairman?

Q179 ***Chairman:*** Yes.
Professor Hutton: At the end of 2006 there were 16,038 volunteer samples on the National DNA Database, and that represents 0.43 per cent; and 99.14 per cent were criminal justice samples. But we have to add that not all those people were subsequently convicted of an offence, they were people who have had a sample taken because they were detained at a police station. There is a small number of what is called casework records, which are different samples, which is another half a per cent.

Q180 ***Lord Rowlands:*** But is that figure because they have just got round to putting it on the database because it is costly? We heard some evidence from the police last week that it is a costly business. Is it default

rather than by deliberate intention not to put it on the National Database?

Professor Hutton: As I understand it the admission to the National DNA Database—and I may be wrong on this and this is one of the things I am looking into at the moment—is under the ultimate control of the custodian of the database and not all samples which are sent are placed on the National Database register. I have to say that the situation that exists is outside any national regulatory framework and has many elements of judgment in it. If we look, for instance, at the law relating to this, as far as we were able to ascertain in our committee—and we spoke to a number of legal people—although the police can take samples and load them on to the database there is actually no compulsion on the police to take a sample when somebody is arrested, and once arrested and the sample has been taken there is no compulsion for it to be loaded—it is entirely at the discretion of the police.

Dr Wallace: I have some figures here that might be helpful, based on a Parliamentary question about the numbers of people on the database at the end of June 2006. They are estimates because I have recalculated the numbers assuming the replication rate, which was subsequently given—there are copies of some people's records—which is now estimated at 13.7 per cent. There were 605,000 roughly who were un-convicted people with a Police National Computer record which had no record of conviction—some of those people would have been awaiting trial. There were 1,681,000 who had received non-custodial sentences or cautions—so that is the largest group of people. There were 636,000 people who had a custodial sentence recorded on the Police National Computer. Then there were a further 429,000 people with no Police National Computer record, and that included approximately 18,000 volunteers. So volunteers are around about that number of people but they occur in a context where there are around one million people on the database who do not have a record of conviction at that date.

Q181 ***Lord Lyell of Markyate:*** I am going to go to question six, my Lord Chairman, because I think it does slot in. The Nuffield Council on Bioethics' report suggested that suspicion of involvement in a non-recordable offence does not justify the taking of bioinformation from individuals without their consent. How can we draw the line between offences that justify taking bioinformation from non-consenting individuals and offences that do not justify such a course of action? And can I ask you perhaps to tie this in with the well known illustration of the Soham murder case where Huntley had been arrested, I think, or at least been in police stations prior to that and if the information had been available it might have assisted in clearing that case much earlier. What is your answer to that question, of which we gave notice?

Professor Laurie: In answering that question, my Lord, can I go back to the fundamentals that frame the Working Group's report, which is that the starting point is fundamental rights and freedoms, liberty and, in this context, consent also, autonomy and respect for bodily integrity, and a need for justification if we depart from those principles, which must be shown to be necessary and proportionate. The specific recommendation that we gave was when we were talking about circumstances where somebody is under suspicion of a non-recordable offence, an extremely minor offence, and when they have not given their consent; if you compare that with the current situation that exists in law it is the case that all arrestees, without their consent, regardless of the reasons of arrest, can have samples taken and those samples will be retained indefinitely. On the basis of the approach that the Working Group actually applied we felt that that was disproportionate given the fact that it was so minor and it was only as a matter of mere suspicion. Matters may change if somebody had been charged, for example, with the particular crime—at that point that might tip the balance towards the justifying of the taking and retention of the samples—but what we are pointing to here is almost a *de minimis* position whereby we feel that it is not proportionate to do that given the consequences. To tie it to the Soham situation, it would depend on the circumstances in which that person had been detained, whether he was ever charged with something. Perhaps another relevant factor might be the fact that he had been detained on several different occasions; these may all be factors that are weighed in the balance. The fundamental position that we are really reaching for in the report here is to say that the onus is on the state to justify when it is necessary and when it is proportionate, and that is necessarily a very vague concept; but what we have to put in the balance are relevant factors. Possibly one issue that is relevant is trying to draw a distinction between offences that are recordable and those that are not recordable. At the moment we suggest that the way in which that division is drawn in England and Wales is arbitrary and is not clear, but what we would call for is broader discussion and debate about whether that device of trying to draw a line would be helpful in trying to decide what sorts of interventions would be justifiable and which ones would not be, based on the type of offence. But it may not be ultimately a useful device; at the end of the day it is simply a device.

Dr Wallace: I just wanted to draw the Committee's attention to the example of the debate in Scotland where extending the law to match England and Wales was fully considered by the Scottish Parliament and the vote in the end was to adopt a compromise which

required the removal of people's DNA profiles and the destruction of their samples on acquittal or on the cessation of proceedings, except in some specific circumstances and those circumstances were that a person had been proceeded against in connection with a serious violent or sexual offence and that in those circumstances the police could request retention after acquittal, initially for a period of three years and if they wanted to retain the data longer they had to apply to a Sheriff for an extension to that time period. I am not saying that that is necessarily exactly the right balance—I think it is very difficult to reach conclusions on that issue—but it was an attempt to come to a decision based on proportionality about the retention of data from some innocent persons in some circumstances but with judicial oversight.

Q182 ***Lord Lyell of Markyate:*** The dilemma is this, I think, that the numbers that Dr Wallace gave us show that all those people who are on the database who are often referred to as the active criminal population actually include something like one million people for whom that would not be a fair description at all. On the other hand, if one was as strict as Professor Laurie is saying then all that information about Huntley would have been lost to the police; am I right?

Professor Laurie: An additional factor that was important for the Working Group was the fact that there is not convincing evidence at the moment that in respect of the types of crime we were talking about, in that example that you gave, retention of those people's information indefinitely would actually further the ends of justice. If there is evidence that can be brought forward to justify that sort of retention then that would obviously be more acceptable, but at the moment we do not see that evidence.

Dr Wallace: Can I add that in relation to the Huntley case—because I think it is a very good illustration of what data you need to keep and what you do not—one important issue to remember is that Huntley was not identified on the basis of a match on the DNA database, and indeed that is extremely rare in murder cases for a cold hit on the DNA database; in other words, someone who is not already a suspect from whom DNA cannot be taken. So DNA was very important in that case but the existence of a DNA database was not necessary or relevant to solving the case. The issue about retention of data related to the Police National Computer records is where it was argued that if those records had been kept Huntley may have been flagged up as a person who may be a risk to children and therefore may not have been given a job working as a caretaker in a school. So there are two issues there about the types of data you retain and how they might be used. I think the second issue is really; does that mean that you need blanket retention from everyone who is arrested in order to catch those kinds of cases? And I would argue that you do not and that in fact you do not gain any significant added value by expanding the database so significantly.

Q183 ***Lord Peston:*** I want to make sure I understand. Is the essence of your position that there is something special about bioinformation as opposed to all other information you might ask people? Is that the essence of what you are saying? So, for example, it is reasonable to ask, "What is your name?" if you are involved with crime, "Can I see your driving licence?"—you regard all that as non-fundamental. But if I say to you, "I really want to know the one thing that will identify you, namely your DNA," then I have got myself into a fundamental ethical question. For somebody who has spent his life studying ethics as an economist you have lost me; you have completely lost me as to why this one piece of information, which just happens to have a very good scientific foundation as opposed to almost all other bits because I could lie about my name and all sorts, am I right that you are saying this is so fundamental that it requires ethical committees, it requires regulation with regulators, it requires control and everything else under the sun. If I were to ask you your name and you would not tell me I would assume you were crackers, not that you were defending your human rights. It is the fact that it is bio that is driving you?

Professor Laurie: It is interesting it is the fact that it is bio and we must remember that this report comes out of the Nuffield Council on *Bioethics*—it has this remit. The Council took a very cautious decision to focus its report on two issues, DNA but also fingerprints, but in certain aspects of the report when it comes to regulation we actually do make recommendations saying that there are many other types of databases such as palm prints, footprints, face recognition, iris recognition, which are also incredibly valuable for the social ends that we are concerned with in the context of crime and that they also require proper and robust regulation and that there may be additional concerns if they are linked. So I would not say that we are arguing for a special case for this, it is just that it is particularly acute at the moment in terms of what is required and what has been happening.

Dr Wallace: I think it is useful to think about the purposes to which this information can be put, so there is a difference between DNA and fingerprints and other biometrics, such as iris scans, in the sense that someone could come into this room and look for our DNA and fingerprints after we had left, in other words it is a tracking technology, a technology that can be used to follow you wherever you go. In addition with DNA there are some specific properties of DNA which allow you to determine paternity,

non-paternity and relationships and also if you analyse the sample, as we heard, some health information. Finally, I would like to point out that there is an issue about the retention of names; there is an issue about the retention of the Police Computer records, the decision to retain those was taken on the basis that the law had already allowed retention of DNA and that in order for the police to know at the police station whose sample has been taken they needed those Police National Computer records. A corollary of that is that we now have for the first time in British history a permanent record of everyone who has been arrested for a recordable offence. That has privacy and civil liberty implications.

Professor Hutton: Just to add some comments as an individual and not speaking as the Chair of the Ethics Group, you asked the question, my Lord, is there something special about DNA? I think that you can answer yes and you can answer no. It is useful perhaps in terms of trying to get a handle on the emotional aspects of it to look historically, just over the past ten years. DNA profiling or DNA fingerprinting is undoubtedly one of the key advances that the criminal justice system in every country has made in the prosecution of crime and in its detection. The problem is where do the rights of individuals lie against it? In the early part of the development of DNA, which I would categorise from, say, 1990 to 1995, there was without doubt at that time a belief that it was going to be the best biological marker. However, it has a number of severe downsides, the most serious of which, in terms of practical policing, is that it takes at least a day to get a return. In the intervening period of time things like iris scanning, which Graeme has mentioned have come along, and there is better computer recognition of fingerprints, which incidentally will distinguish between identical twins. I think that had iris scanning come first then the concentration on DNA collection would not have been as great. If you couple that with the concerns of a number of groups in society relating to the so-called surveillance society, and a comment from our previous Prime Minister that everybody should be on the database, then I think for people who are so minded it creates the impression that the collection of excessive data has an occult motive. I think that is the point of distrust.

Q184 ***Chairman:*** What motive, professor?

Professor Hutton: An occult motive or some sort of malevolent surveillance motive. I think it is most easily understood in an historical context of the last ten to 14 years.

Q185 ***Lord Peston:*** So you would reject totally the suggestion that the concentration on DNA is just the latest example of the anti-science lobbies in our society? You do not accept that?

Professor Hutton: I do not accept that, no. I am trying to present a balanced picture.

Q186 ***Lord Peston:*** I understand that and I am very sympathetic to the need, and that is what this Committee is doing but I want to know who is driving what.

Professor Hutton: I think the concern about DNA specifically is characterised not by its criminal use for identifiable criminals, the concern is characterised by its potential use against people who are not criminals and uses which extend beyond that of forensic identification.

Q187 ***Lord Morris of Aberavon:*** I will resist the temptation of chasing quite a few hares, as I would like to. Dr Wallace, you have raised this spectre of the possibility of misuse and there is a real and imaginary fear of big brother, and we are back to priest holes, lock up all the chapels in remote areas, major generals in Cromwell's time, right down to the interests alleged, to MI5 and the miners' strike. The line must be pretty thin, I would have thought, between proper investigation and interests and that which would be improper. How can it be corrected?

Dr Wallace: I think it requires a range of safeguards and there is no single measure that is going to prevent misuse. I think for us one of the key safeguards is the issue of time limits on retention, the removal of innocent people and also time limits perhaps on retention of data from people convicted of minor offences. The reason for that is precisely the point that you raised, so for example I postulated the scenario of police coming into this room after we finished and it is very difficult to devise legislation that would distinguish between us sitting here discussing this issue or us sitting here plotting a terrorist act, so it is very hard to write legislation that interferes with one type of investigation and not with another. I think what you can do is to look at the database itself, and perhaps more broadly also at linked databases with other data, and say that it is unacceptable in principle for permanent surveillance or permanent retention of data to be implemented without any judicial oversight. The implications of that may go much broader than the DNA database but in the context of the DNA database itself we would say that we need specific legislation to govern the provision of the database and that that includes conditions on the retention of people's DNA profiles, and, we would also argue, the destruction of the samples themselves once an investigation is complete.

Professor Hutton: To add information to the discussion (as opposed to my personal opinion) if one speaks to a number of the people in the criminal justice system about the wisdom of taking samples from everybody who is arrested or detained at a

police station the answer which one gets is that crime runs in families. Crime is repetitive within individuals and families and you may as well get the sample as soon as you can—that is a form of thinking which has, shall we say, informed decisions in this area. The downside to that is that it is, as far as I know, completely unknown how many people whose samples are on the National DNA Database because of an incidental event which led them to a police station, subsequently go on to commit another crime. That is a piece of work which we in the Ethics Group are going to commission from the National DNA Database, to try to establish whether or not there is any genuine forensic value in taking a DNA sample from everybody detained by the police.

Q188 ***Baroness O'Cathain:*** That neatly takes me to the question I was going to ask, whether you see the over-representation of some social groups in the National Database as a problem in terms of ethics, human rights or social cohesion? As a corollary to that, this actually is the concern that a lot of us have, and a concern that makes people willing to suggest that perhaps there should be a universal DNA database. Similarly, the point you have just made about concerns that families, etcetera, have an inbuilt propensity to crime seems to be completely haywire to those of us who are not close to it. So how do you think this is a problem?
Professor Hutton: Could I say that when I made those contributions to the Committee I was rehearsing other people's arguments.

Q189 ***Baroness O'Cathain:*** Yes, of course.
Professor Hutton: If we briefly review how we got to the current situation. The Criminal Police and Justice Act 2001, section 82, allowed the indefinite retention of samples from criminal justice profiles. Prior to that, if a profile was on the database it was removed and the sample destroyed once the case was closed if you were not guilty. So 2001 was the point at which when somebody had a sample taken and it went on the database it stayed on. Section 10 of the Criminal Justice Act 2003, allowed the police to sample at their discretion for all recordable offences. That is what resulted in the huge increase in numbers on the database. At the moment there are some groups who are hugely over represented on the database in relation to their population incidence in society in general. A particular group is black youths. However, we in the Ethics Group intend to make a proper study of this in the future. We have done some preliminary work and the preliminary work would suggest extremely strongly that the reason for the over representation is directly related to the stop and search policy which is occurring in community policing, and once somebody has been in a police station the DNA is taken automatically. So we would see the current representation and social sectoring of the National DNA Database as being (from our initial results) a direct reflection of the fact that the Criminal Justice Act 2003 allowed everybody who was detained, whether they were guilty or not, to have a DNA sample taken.

Q190 ***Viscount Bledisloe:*** You talked about over representation in terms of their proportion of membership to a society, but it is inevitable, is it not, that if we are talking about people who have committed crimes or are suspected of having committed crimes that certain groups will be disproportionately represented. Young men commit a great many more crimes than young woman, and there are various other groups. So you really have to compare surely not with their proportion in society but with the proportion of them who are in fact convicted?
Professor Hutton: I agree with that. What I would say is that that is a piece of work we are intending to do and at the moment our preliminary results would suggest that your thoughts were heading in the right direction and that the relationship with numbers and proportions was directly related to the number of people who are arrested or stopped and searched. I think the social concern, if I can add one thing, from some groups, is at the very basic level of policing there is a disproportion in relation to the groups who are stopped.

Q191 ***Viscount Bledisloe:*** That I fully accept, yes.
Dr Wallace: Can I just distinguish between those causes, which I am sure are being investigated, and the consequences of dis-proportionality because I get a lot of phone calls from people on the database, many black men who say that they feel their DNA has been taken for racist reasons and so on, grandmothers whose 12-year old grandchild's has been taken because the neighbours falsely accused them of damaging their fence, and a wide range of stories of this kind, and I think the problem that I see from those phone calls is really that people's sense of fairness and their trust in the police is being undermined. So whatever the causes are I think people feel that, "If the police accepted that I did not do anything wrong . . ."—as in many cases—". . . and they apologised to me, the neighbour was making a false accusation, and my grandson did not do anything, then why does the data have to be retained?" That is what we see. And we also hear this from some police officers who are concerned directly about the implications for trust within their communities.
Professor Laurie: I simply want to point out that the figures are actually quite alarming, and certainly the ones that were given to us, because we understood that one-third of young black males are on the

National DNA Database compared to one-eighth of young white males.

Q192 ***Viscount Bledisloe:*** I am not saying there is not a disproportion but what I am saying is that you could not possibly take it across the population as a whole because if there were the same number of widows of 80 on the database as there were of young men of 18 to 20 it would be a pretty useless database.
Professor Laurie: But that does not reflect the numbers that are actually guilty of offences on the basis of arrest, which is the concern.

Q193 ***Viscount Bledisloe:*** I accept that.
Dr Wallace: Something like 77 per cent of young black men under the age of 35 are on the Database, so clearly that does not reflect the numbers that have actually committed crimes.
Lord Lyell of Markyate: Just briefly in this context, we have a distinguished colleague in Parliament who, I think on the floor of the House certainly makes no bones about it, was a special constable working in Central London for quite a period and he said that the chances of a young black male going in a motor car between, say, Euston and Brixton and not being stopped probably more than once were very small.

Q194 ***Baroness Quin:*** Just to ask you, does black include black and Asian?
Dr Wallace: The figures are somewhat uncertain because the categories on the Police DNA Database are based on appearance to a police officer and in order to get the figure you have to compare that with the census figure based on self-reported categories by the individual. So it is an estimate. The categories that are written on the database are not based on the individual's perception or reporting of their ethnicity.

Q195 ***Lord Peston:*** I think my question has been answered. I think I would be right in saying that either because it would be a waste of money or that there are ethical questions you would not favour a universal DNA database. As a matter of interest, wearing my economics hat, the cost involved is massive, is it not?
Dr Wallace: Yes. It would be something like £1 billion just to do the analysis for people actually living in the UK, let alone the police costs and so on and so forth.
Professor Hutton: If I could just make a comment? Again, following the sentence which I read out earlier from the Ethics Group, I think there is an extremely cogent argument that could be made—I am not saying I necessarily agree with it but I am sympathetic to it—for the government of our country being able to identify unambiguously everybody who was living here and the people who are travelling in and out. Those civilian requirements, which can be argued to be for the benefit of society, would produce a very different type of identification methodology than those in which you are trying to establish an identification methodology which is related to the deposition of human tissue. So I think that when people have made the assertion that it would be a good idea to establish a National DNA Database—and I try and put myself in their minds—I think they probably were not aware of the other ways of identifying people and I think they were possibly unaware of costs of DNA in relation to other techniques. The arguments about whether or not there should be a civilian repository of information which identifies everybody are different and fundamentally different to the arguments as to whether or not there should be a criminal repository.

Q196 ***Baroness O'Cathain:*** May I just briefly follow on from that? There is no information at all in the public domain—at least I have never seen any—on this point that you made, that there is an alternative to identifying everybody in the country other than the tissue one, the DNA.
Professor Hutton: Absolutely.

Q197 ***Baroness O'Cathain:*** Somebody somewhere ought to inform the public about this because there is likely to be a constant demand for DNA to be universal, for the National DNA Database to be constructed for everybody in the country.
Professor Hutton: What I hope we will have stimulated by our report, which went on the Home Office Web yesterday, is the possibility that there should be a debate about that and that there are alternatives—they are cheaper, they are quicker and they are as reliable.
Dr Wallace: Just a small comment on the practicalities. I am sure you know my opinions on the downside but *Computer Weekly* reported—and I am not a computer expert—that this would require a storage area network the size of Belgium in order to store all the data that you would require for DNA collection. So I just want to say very clearly that I think this is a red herring. However difficult the decision is about who should be on the database and who should not be it is a difficult decision that has to be weighed up on that smaller ground of proportionality, and talk about everyone going on the database is really not a practical solution.

Q198 ***Lord Morris of Aberavon:*** It is mentioned in the Nuffield Report, Professor Laurie, that the present regulatory structure is piecemeal and patchy and that there should be a statutory framework. How could that be done? Would it be different to the Interception Commissioner's report, which we read

yesterday, from Paul Kennedy, a very distinguished former Lord Justice of Appeal? I presume it is not statutory. Would it be something of that kind or something more formal?
Professor Laurie: The thinking behind this was as follows; that it was actually incredibly difficult to get hold of some accurate information when we were putting the report together about what was actually going on with all of the reforms because various different agencies were addressing different issues at the same time. There is also the evolution that we have seen in terms of the development of the law in this country, to which Professor Hutton has taken us to some examples, and we now have multiple pieces of legislation which need to be fitted together in order to understand exactly what is going on. But it became apparent to us in our discussions that what is missing is independent, accountable and powerful oversight; a fundamental reappraisal of the basis of the National DNA Database; a suitable framework for its development, its management and governance—which is not actually in law at the moment—clarity of purpose and also articulation of the values that actually underpin this, which are lost in this morass of laws; and we came to the conclusion that consolidation of this entire field of law would seem most appropriate. The particular way in which that would look is obviously up for discussion but we do offer a couple of examples in our report—I cannot comment on the report you looked at yesterday—and we do give the examples of the Independent Police Complaints Commission and also the Human Fertilisation and Embryology Authority, both of which have statutory powers and have responsibilities and public accountability, clear powers of action, independent oversight and also criminal sanctions for non-compliance with the principal provisions of the legislation; we feel that the sort of exercise of looking at what are the fundamentals at stake and all the issues that have to be addressed here, particularly if we look to the future and consider that there may be linkage across different types of database beyond DNA, then what we require is a more holistic approach within a clear framework. And whilst we were very pleased to see the establishment of the Ethics Group we had lots of questions about what its powers were, how might it actually operate, what could it actually do in terms of sanctions if it disapproved of the way in which the National DNA Database was being run? We feel on balance that that would be best addressed by statute. The alternative is regulation by consent, which is fine as long as the actors give their consent and comply, but this area may be too sensitive, the needs for public trust and confidence may be too great, and the threat to civil liberties may be too significant to leave that to such an informal and imprecise process. So that is what informed our thinking.

Q199 ***Viscount Bledisloe:*** I think you said, Professor Laurie, that one way to do this was consolidation of the statutes. Do you mean consolidation in the technical sense when you just draw together all the Acts of Parliament in one Bill without changing them, or do you really mean a fundamental review of the law to bring a sensible, coherent whole into one Act?
Professor Laurie: Thank you. I obviously mean the latter in the light of our discussions this morning.

Q200 ***Lord Rowlands:*** I would like to address my question to Dr Wallace, if I may? I am going to ask you what changes you would like to make to the Data Protection Act and you mentioned constitutional safeguards and constitutional committees and we welcome any suggestions you might have on the constitutional side, but just before that in your written evidence you quite frequently refer to individuals whose records are on this database and who are suffering hardships in daily life and employment. Let us take an example of employment, do you have any actual examples where people have either lost jobs or not got jobs because they have been on the DNA database?
Dr Wallace: No, I do not. This basically relates to the retention of the Police National Computer records and there are examples certainly of people with convictions for minor offences in the distant past; there are some cases that are coming to the Information Tribunal.

Q201 ***Lord Rowlands:*** This is not in the DNA sense?
Dr Wallace: No, it relates to the retention of the records on the Police National Computer. That decision was not directly taken in the 2003 legislation but it was a decision that followed from it in order to keep those records so that the police had access as to whether or not they had already taken a DNA sample.

Q202 ***Lord Rowlands:*** So when you make statements that people's employment prospects could be diminished by being on the DNA database you have no evidence of that at all?
Dr Wallace: No, it is a consequence that flows from the link between the two databases, so the criminal record or the record of arrest of the individual is kept on the separate database, which is the Police National Computer. Those records are now being permanently kept in order to match with the DNA records; those records can be accessed under enhanced criminal record checks, for example, and can be lawfully used to refuse visas and so on, for example. We are not aware of that happening at the moment but it is certainly a real possibility because there is no legal protection that would prevent it.

Q203 ***Lord Rowlands:*** But an employer cannot access the DNA database in any shape or form?
Dr Wallace: The employers and the police themselves cannot access the DNA database directly.

Q204 ***Lord Rowlands:*** Then what type of changes do you want to make to the Data Protection Act and what constitutional safeguards do you want us to put in place?
Dr Wallace: I would agree with Professor Laurie that what we would like to see is legislation—the operation of the database put on a legislative basis. Current law in relation to the database only covers the circumstances under which the police can take samples; it allows indefinite retention and it restricts the uses under this in rather broad terms. We would much rather see legislation that specifically governs the operation, setting up the proper oversight, time limits and so on in the context of the DNA Database itself. However, there is a broader issue which of course you have just raised in relation to other databases, the links and potential future links of different databases, and that links with the constitutional issue. There is an issue here about the permanent retention of data from citizens that have been collected for the purposes of investigation or surveillance and whether that data should generally be allowed to be kept permanently in order to make that person, in effect, permanently under bio surveillance, or potentially, in terms of wherever we go, and that is the area where we think some kind of additional protection is needed to say that that is not acceptable without the individual's consent or without some kind of judicial oversight of the uses of that data.

Q205 ***Baroness O'Cathain:*** The Nuffield Report raised concerns about the integration or linkage of forensic bioinformation databases with each other or with other databases, possibly through the IDENT1 database of fingerprints. Could you please explain these concerns and estimate the likelihood of such integration or linkage within the United Kingdom? And how would that link in with the proposal for identity cards?
Professor Laurie: The Working Group was not led to believe that there were any immediate plans to link bioinformatics databases but if you look elsewhere the phenomenon of database linkage is prevalent; we see it across all sectors from social work and housing to healthcare and medical research, and what we wanted to do is look to the future and the possibility of what might be required if any such linkage was one day possible. As I have already said previously, there is now a proliferation of bioinformatics databases which potentially could be linked up. The argument in favour of this is that the power of the totality is so much more than the sum of the parts, but with that increased power of the super database, as it were, comes increased concerns about privacy and liberty of exactly the same nature that we have identified already this morning. I think in regulatory terms an overarching concern at the moment is that these different databases which may be linked up are not regulated consistently in any way, shape or form and we therefore have a considerable variation across issues of quality, retention times, exchanges of data between other bodies internationally and also who would have access. So what we would hope would happen would be to look to the future and consider what are the possibilities, which may actually be justifiable in due course, but also what is required to be in place before those possibilities became realities. Because another possibility, linking into the second part of your question, would be that it may be thought to be valuable at some point to link some information on these databases to other types of non-forensic databases. But, again, going back to the fundamental principles that informed our report, would that be justifiable, would it be necessary and would it be proportionate for those social ends that ID cards are supposed to serve, as opposed to the criminal ends that the DNA Database and others are supposed to serve?

Q206 ***Baroness O'Cathain:*** Surely ID cards are also supposed to serve the criminal elements as well; that is the rationale for them, is it not? anti-terrorism and all the rest of it?
Professor Laurie: Indeed there can be overlap, but they are also linked very much to social services, and it is in that argument that there can be overlap that we can see arguments emerging that there is a case to be made to link the forensic to the non-forensic.

Q207 ***Baroness O'Cathain:*** In terms of the database, there are more databases than the ones you have actually mentioned?
Professor Laurie: Absolutely.

Q208 ***Baroness O'Cathain:*** Is the general public really aware of the number of databases that there are and is there a case for making this information universally available? For example, if you go to any Interflora, and you ask for flowers to be delivered, you are first of all asked for the postcode and then you are told the name. I find that quite incredible. Everything we do seems to be on a database somewhere, so why are you against more information? It is easier to have them all over the place and the risk of having CDs on the roundabout outside Exeter airport is lessened.
Professor Laurie: The consequences in a criminal justice setting can be quite significant compared to the consequences of the florist having your name and address and we would really have to consider very

closely on what basis there would be a case to link those types of very separate databases together in the first instance.

Professor Hutton: If I could make one or two comments? I absolutely agree with Professor Laurie that there should be a better statutory basis, and that is argued in the Ethics Group papers which are now in the public domain. The question, Lady O'Cathain, that you asked about information, I think the logical way through it, or the approach which we are taking—and I do think it is a very pertinent question to current society—is that the country has agreed to be subject to the Human Rights Act. Article 8 of that Act, which relates to privacy, requires an intrusion into privacy to be based on three tests: is there a legitimate aim to the interference of privacy; is the interference prescribed by law, and is that law accessible; and is the interference proportionate to the identified aim? In order to answer those questions I think there needs to be a structure describing types of personal information and what we are likely to propose—although I cannot say this definitely because we have not yet had the meeting about it—is a way of thinking about information that may differentiate the personal from the custodial. We will probably propose that there should be four types of personal data recognised. The first would be personal data held on military, specific governmental and other specified personnel, which was required to be held in order for that person to carry out their job. In terms of the military, for instance, you might need DNA because they may die and you may need to identify them. In my case, as a person who deals with many blood products from day to day it is very reasonable that it should be known within my employment what my infective capability is in relation to Hepatitis B. So that would be data within a contract of employment. The second type of personal data which could be held would be data held on criminals and others guilty of antisocial behaviour and the justification for holding such data would be the prevention of disorder or crime or the protection of health or morals, on the basis that it safeguards the rights and freedoms of others and ensures public safety. It is in that category that we would have criminal information. The third section would be personal data which would be held on law abiding citizens that enables society to function properly. Examples of that will be personal identifying numbers, such as the national insurance number, birth, marriage and death certificates, bank account numbers and passport numbers. Without these it is not possible to run a legitimate society, and the justification for the intrusion is that it allows society to run smoothly. Then finally there should be personal data not in any of those categories which is truly personal to the individual themselves and it is up to them if they choose to release it.

Q209 ***Lord Peston:*** I want to come in on the last point. Everything you say is a very sensible and logical thing except that with regard to the last category the individual seems to want to have it both ways. I am thinking of film stars and all sorts of public figures—they want privacy on their terms, therefore they are anti the investigative press and everything else under the sun. You can argue that in a free society that your rights to stop me finding out things about you do not necessarily override my rights to find out things the other way. Certainly if you talk to any journalist they will argue that. Particularly if you recognise the existence of Google, you type in the name of anybody in this room—and I was staggered about the number of hits that came out about me because I thought my days had long gone, but they are there because I am putting them there, if you like, in a way. It is that last category which all the other things you said are completely unobjectionable, it seems to me, but that last category is, I believe, in freedom on my terms but not on anybody else's terms is close to the proper functioning of a free society. So the last one seems to be at least debateable.

Professor Hutton: Could I suggest that in the arguments you put—and I do not want to be critical—I think you may have mixed different parts of information. If we were to return briefly to these four categories, there are the things you need for employment, the things about criminals and the things we all have to do to make society run and then we are left with our own information. This suggestion, which we will probably bring forward, is currently not enshrined in any legislation; if it were it would be easy to categorise things. The issue of information on the Web, if you Google my name you get plenty of hits, most of it is information which is absolutely freely available—it relates to my employment, it relates to talks I have given, it relates to things like this where I have made a particular comment—it is in the public domain. I am pleased to say that you will not find anything in there about my health or my personal life. That is my actual own information. I think the issue of public figures—I prefer to call them public figures rather than celebs—is at what point—and this is slightly off the DNA agenda—is there a justified public intrusion into an individual's normally personally held data? I think in my particular position if I were seen to be doing odd things at work it is appropriate that my employer and possibly some members of the public who act as lay people should enquire as to why that is occurring, and on the basis of the benefit to the public it may become known to a limited number of people that for instance I might be suffering from depression. I think it is appropriate then that that group of people who are responsible to the public should know that about me. I think the issue of celebs, as we call them, and the

intrusion into what is newsworthy, there has to be a line drawn. Is it really in the public interest that if somebody is wearing a flowing skirt that the public should know that they are pregnant or whatever? I think that is completely different to the sort of issues that we are talking about with DNA analysis and should not be confused with it.
Lord Peston: I understand the point you are making.

Q210 ***Lord Rowlands:*** *Facebook*, that is where you volunteer to give up your privacy.
Professor Hutton: Correct.

Q211 ***Lord Rowlands:*** Is it in that category?
Professor Hutton: What I said here was that personal data not included in the above categories—so that is the things you have to give—is truly personal data over which an individual has total control and an intrusion into this, or the holding of it by another person, government agency or commercial organisation is an offence under Human Rights legislation in this country unless specifically permitted by the individual. Whatever information you put into the public domain by your own volition essentially removes its confidentiality and hence you cannot stop people using that information subsequently.
Lord Peston: To take an obvious example, one of the great databases we have is *Who's Who?* to which you put in. I can still remember my late, much missed friend Lord Carter in the old days, when we were listening to people in our House lauding the values of family life and he would get it out and he would say, "How many times do you think he has been married?" and that gave you a perspective. He may not want you to look at that data and may have left it out but it is not exactly outside the public interest that those who laud the value of marriage might well abide by marriage.

Q212 ***Viscount Bledisloe:*** Is this interesting discussion within the scope of our inquiry!
Professor Hutton: Just this one point. I do take your point and I think it would be appropriate if somebody holds a public office that there should be a statutory agreement as to what they will disclose.

Q213 ***Lord Lyell of Markyate:*** Can we go beyond these shores? The Prum Treaty of 2005 is a cooperation agreement amongst a number of EU Member States which does not include the United Kingdom, but provides for mutual access to DNA databases, and there are other provisions, including Interpol and Europol, which could reinforce cross-border exchanges of bioinformation. Professor Laurie, the Nuffield Report shares the concern expressed by the House of Lords EU Committee in 2007 and endorsed its recommendations—and I would like an explanation here—for transparency and evaluation—I always wonder what transparency means—if the Prum Treaty were to become an EU instrument. Could you please expand upon the threats that these developments pose, specifically to citizens of the United Kingdom? And could I just add, because I always worry about it, the EU arrest warrant?
Professor Laurie: As my previous answers have indicated the Council's report does not believe that the governance methods in the United Kingdom are sufficiently robust to strike the appropriate balance in terms of the uses to which bioinformation can be put, and I think therefore one can easily imagine that if information about UK citizens is sent beyond our shores to other jurisdictions where the standards may be higher but may be lower and we lose all the more control then that would be a point of further concern. I think also in terms of the issue specific to UK citizens, given the fact that we have the lowest threshold in the European Union for admission to a DNA database and we have the highest number of citizens on our DNA database, it means proportionately that more UK citizens could have their privacy invaded by international transfers compared to other countries within the EU. Our recommendations basically endorse what the House of Lords' European Union Committee also suggested, which was that we require robust and regular monitoring of the uses or the reliance on the Prum Treaty, and that is where the issue comes in about transparency—that if you have regular monitoring through public reports you can at least ask the questions of what has been done to whom, for what reasons and how was it justified. Secondly, we argue that really before this should be adopted we require to ensure that the data protection protections around the European Union are of an appropriate standard. Actually data protection legislation may be something that can inform Professor Hutton's group in terms of the recommendations about personal information because there has been a lot of discussion around those issues recently, but one of the concerns is that at the moment in the context of what is called the Third Pillar of the EU, which deals with police and judicial cooperation in criminal matters, there has not been sufficient investigation about the levels of data protection, and there are concerns in respect of, for example, disparate legal regimes, disparate collection and retention schemes, disparate approaches to access, that mean that concerns we have in the domestic context are exacerbated in the European and international context. In relation to the EU arrest warrant, yes, if we make arrest the threshold criterion for entry on to a database and if that is thought to be an acceptable idea elsewhere then it may all the more exacerbate the concerns that we are expressing this morning about

the fact that that is probably not enough to protect the civil liberties of those who then go on to these databases on a permanent basis.

Dr Wallace: I just wanted to add that we often use the phrase "big brother" but I think what it really means is that we are happy with databases that have the bad people on them and the good people watching over that, but we are concerned about databases that have the good people on them and the bad people watching over them, which in the extreme is of course the Nazi government. If you expand access—and I do not want to be specific about it being to Europe, it may also be about having an increasing number of labs, it may be about increasing collecting DNA on the streets, which was another proposal—you increase the possibility of infiltration to that system. So the worse case scenario is a scenario where you have somebody trying to track a child not because that child has been kidnapped but because they are a potential abuser of that child. I think it is unlikely that there will be direct access to the database—direct access is not allowed to our own police—but there is a scenario in which DNA from a toothbrush is used to trace an individual, which is a common use of this type of database. If somebody can do that who you cannot trust then you want to be very worried about it.

Q214 ***Viscount Bledisloe:*** Professor Hutton, very briefly, the role of your Group, what is to be the status of its advice; and will you have real power to see that its recommendations are implemented?

Professor Hutton: The Ethics Group had a gestation period of about five years, since it was first suggested. It has gone through a variety of putative forms on the basis of these suggestions. When I was appointed as the chairman of it it was intended that it should be a sub committee of the National DNA Strategy Board. I argued at the time—and I must place on record that I was supported by ACPO and the Home Office—that this was an inappropriate relationship between the Ethics Committee, which was meant to be representing the public and the arrangements in the DNA Strategy Board. Subsequent discussions converted it into a non-departmental public body and that was presented to Parliament by Meg Hillier on Wednesday 25 July last year. The protocol governing the Ethics Group, which I can send in, states clearly that it will act independently, that it will advise Ministers and that although it will carry out its discussions in private the minutes of its meetings will be published subject to any redactions that were considered necessary by the Home Office. The gentlemen's agreement on that was that the redactions would simply be to prevent individuals being identified and to prevent any intrusion into existing legislative procedures. We have had two meetings; both sets of minutes have been posted on the Home Office website without redactions for everybody to see. I think I would say that the situation that currently exists is that ethical and moral decisions which inform legislation by their very nature have judgments surrounding them. We place our notes in a very full format, as we have done on the web page, so that people can see how we have come to our recommendation. It is advice for Ministers and it is also there available in public to people who disagree with it or wish to take a different judgment call on the evidence that we have produced and who wish to argue it in public. So we would see ourselves as providing advice to Ministers but similarly also to people in other parts of the governmental process, giving them the rationale why we give that advice and giving them the opportunity, if they so wished, to put a different interpretation on it.

Q215 ***Viscount Bledisloe:*** If your advice is not taken up by the Minister you will be dependent upon somebody else, say a Member of Parliament, taking the issue up to say, "Get on and do this."

Professor Hutton: I would like to think that with well argued text and verbal representations to Ministers that it is likely that things would be adopted.

Q216 ***Chairman:*** Time is marching on, sadly, and a very brief question from me to Dr Wallace, if I may? In its written evidence GeneWatch called for public and Parliamentary debate before new uses of the Database are introduced. Are there any particular circumstances in which you envisage such a debate being triggered; and how would you envisage it taking place?

Dr Wallace: I think to ensure proper Parliamentary scrutiny we do have to have the database on a legislative basis, as I have mentioned. If I can perhaps give an example, there is currently a review of the Police and Criminal Evidence Act going on which proposed expansion to the collection of DNA for non-recordable offences, such as dropping litter and speeding fines, and for that data to be collected in short-term holding facilities outside police stations. My understanding is that the 2003 change to the law, which allowed collection on arrest, also allows the Secretary of State to make changes to PACE that do not go through full Parliamentary scrutiny. That means that we are in a situation at the moment where very significant changes and potentially very controversial changes such as that do not have the kind of scrutiny that they need to have. So I would put that question back to the earlier question about how can you ensure oversight which is on a statutory basis and which does require Ministers to have a proper debate of these issues before they are actually implemented.

Q217 ***Baroness O'Cathain:*** What dangers are there form the other uses to the database and the DNA database, for example familial searching, ethnicity research or commercial activity?
Professor Hutton: Dangers is one word, consequences is another.

Q218 ***Baroness O'Cathain:*** Consequences then.
Professor Hutton: The process of familial searching, which is either mitochondrial searching through the mother's line or Y chromosomal searching through the father's line necessarily does not have the specificity of the multi-component match, about which I was talking earlier. So the consequence of undertaking such a search is that a variety of people will be identified who are some form, probably, of blood relative of the person under consideration or the crime scene. Some of these people may discover they have relatives they did not think they had—I think that is a potential problem. The second thing is that it may result in a member of the family providing evidence which convicts another member of the family, sometimes inadvertently, and indeed there has been a cold case in which that has occurred. So in summary, because we are short of time, what familial searching, (mitochondrial searching and Y chromosome searching) does is to allow a community of people to be identified who may be the miscreant or may be related to the miscreant. In doing that it produces some social events which are unpredictable and may have far reaching consequences, particularly, for instance, in things such as inheritance.
Chairman: Professor Hutton, Professor Laurie and Dr Wallace, can I thank you very much on behalf of the Committee for joining us today and for the evidence you have given. You have been extremely generous with your time; thank you very much indeed.

Supplementary letter from Dr Helen Wallace, Director, GeneWatch UK

I write regarding Home Office Minister Tony McNulty's evidence to the Committee on Wednesday 25 June, in which he made a number of incorrect statements about the National DNA Database. I would be grateful if you would draw the following to the Committee's attention.

In his evidence the minister referred to: ". . . the litany of rapists, killers, child abusers who nominally on anybody's definition would fall into your innocent category, ie they have encountered the criminal justice system but the case has not been pursued against them, only for in some cases 15–20 years later horrendous crimes to be laid at that individual's door purely because of the individual's DNA sample being on the database".

The minister was presumably referring to Operation Advance, a joint initiative between the Forensic Science Service (FSS) and the Home Office Police Standards Unit (PSU). However, the success of Operation Advance is due to the retention of crime scene evidence, not innocent individuals' DNA. During Operation Advance, evidence from crime stains has been re-analysed using the more sensitive techniques available today. Operation Advance III was launched in September 2007. By then, the project had reviewed over 11,000 cases leading to the scientific re-analysis of 423 cases and 116 matches against the National DNA Database. These had resulted in 30 convictions, including four life sentences, and further seven cases were awaiting trial.

The £1 millon cost of Operation Advance is roughly the same as the annual cost of storing the DNA samples of the one million innocent people estimated to have records on the Database, and it is likely to be considerably more effective at solving serious crimes.

Whilst it might be argued that retaining innocent individuals' DNA profiles would increase the chances of identifying the perpetrator in the "unmatched" cases, in reality it is giving the police relatively wide powers to collect DNA, not to retain it, that has provided valuable evidence in some cases. I enclose a GeneWatch UK briefing which provides further information regarding the relevant figures for the DNA Database as a whole. Expanding the number of individuals whose records are retained has increased the expected number of false matches, but has not increased the chances of detecting a crime using DNA. In contrast collecting more crime scene DNA has been effective.

The reference by the minister to Stefan Kiszco—who spent 16 years in jail for a crime he did not commit—is also seriously misleading. Kiszco was jailed in 1976 for the murder of schoolgirl Lesley Molseed on the Yorkshire moors. The forensic evidence which eventually cleared Kiszco was that the semen on Lesley's underwear could not have been his, because he had a health condition which made him incapable of producing sperm—evidence never shown to the defence or court at his original trial. He was freed in 1992, but died a year later. The police re-opened the case in 2001, obtained a DNA profile from Molseed's underwear, and Ronald Castree was convicted of the murder in 2007. He had been convicted within a year of the Molseed's murder of abducting another young girl and trying to assault her, but his DNA was not added to the Database until

2006, when he was arrested for an unrelated crime. The case illustrates the importance of retaining crime scene DNA evidence and DNA profiles from individuals convicted of serious offences, who may re-offend. It did not involve the retention of DNA from any innocent individual and Kizsco was not freed as a result of the retention of either his or Castree's DNA.

In his evidence, the minister stated a number of times that retention of an innocent individual's DNA allows them to be exonerated if they are falsely accused of a crime. However, an innocent individual carries their DNA with them at all times and does not require it to be stored on a database in order to show that it does not match a crime scene DNA profile. The database is used to supply match lists (lists of potential suspects) to the police—not lists of all the persons on the database who do not match the crime scene DNA profile.

Mr McNulty also stated that use of the Database does not involve "fishing" to try to find crimes to attach to individuals. However, use of the Database involves continual "speculative searching" of individuals' DNA profiles against about 800,000 crime scene profiles every year. In contrast, the Police Elimination Database is not subject to speculative searches.

Finally, the minister claimed that people with records on the Database were not a list of the "almost guilty" who might be vulnerable to stigma or discrimination. However, as stated in the National DNA Database Annual Report 2005–06 (page 9):

> "In support of the powers provided by Section 82 of the CJPA and Sections 9 and 10 of the CJA, it has become necessary to retain a nominal record of every person arrested for a recordable offence on the Police National Computer (PNC) to enable a link to be made between the DNA profile held on the NDNAD and fingerprints held on the national automated fingerprints database (IDENT1) to help the police identify and locate an individual following a match being obtained on the NDNAD".

PNC records are available to a wide range of agencies and the information in them may lead to an individual being refused a job or a visa (for example, US visas may be refused on the basis of a record of arrest).

The enclosed briefing (Annex 1) also cites the opinion of the British Academy of Forensic Sciences regarding the disadvantages of creating a DNA database of the entire population, which you may find of interest.

28 June 2008

Annex 1

Would 114 murderers have walked away if innocent people's records were removed from the National DNA Database?

On 17 June 2008, in a major speech on "Liberty and Security", Gordon Brown stated:

> "I say to those who questioned the changes in the Criminal Justice and Police Act 2001, which allowed DNA to be retained from all charged suspects even if not found guilty: if we had not made this change, 8,000 suspects who have been matched with crime scenes since 2001 would in all probability have got away, their DNA having been deleted from the database. This includes 114 murders, 55 attempted murders, 116 rapes, 68 other sexual offences, 119 aggravated burglaries, and 127 drugs offences".

This briefing examines the evidence for this claim and concludes that:

1. The Prime Minister's claim is false.
2. Ministers are well aware that this claim is false.
3. This figure is misleading to members of the public who are concerned about the implications of retaining innocent people's records indefinitely on the National DNA Database.

1. Where the Figures Come From

An earlier version of the figures cited by the Prime Minister was supplied to the House of Lords in the "Marper case" by Dr Bramley, then Custodian of the National DNA Database (NDNAD).[1] Dr Bramley's statistics are summarised in House of Lords' judgment in the case[2]:

> "As at 31 March 2004, the total number of DNA profiles on the DNA database which relates to entries where the parent PNC [Police National Computer] records have been deleted is 162,433. It is estimated that approximately 86% of the PNC record deletions are attributable to subsequent acquittals. Allowing for an 8% replication rate among acquittals (for example, reflecting dual entries through use of aliases, etc), it is estimated that there are approximately 128,517 DNA profiles on the DNA database which would previously have been required to be deleted. From these, approximately

> 5,922 DNA profiles have linked with crime scene stain profiles in respect of 6,280 offences. These offences include 53 murders, 33 attempted murders, 94 rapes, 38 sexual offences, 63 aggravated burglaries and 56 offences of the supply of controlled drugs".

In January 2006, the Home Office released a report which updates Dr Bramley's statistics.[3] It states (paragraph 15, page 6):

> "Since the legal change that took place in 2001, it is estimated that approximately 198,000 profiles that would have previously been removed have been retained on the Database. Of these, at 31 March 2005, 7,591 profiles had been matched with crime scene profiles involving 10,754 offences, including 88 murders, 45 attempted murders, 116 rapes, 62 sexual offences, 91 aggravated burglaries and 94 of the control of supplied drugs".

More recent figures are available in the National DNA Database Annual Report 2005–06,[4] which covers the period to the end of March 2006. It states (page 36):

> "*Matches Involving Profiles Retained under the Criminal Justice and Police Act 2001*
>
> Of the 200,300 or so profiles on the NDNAD that have been retained under the CJPA 2001 and would previously had to have been removed, approximately 8,500 profiles from some 6,290 individuals have been linked with crime scene sample profiles from some 4,000 offences. These offences include 114 murders, 55 attempted murders, 116 rapes, 68 sexual offences, 119 aggravated burglaries and 127 of the supply of controlled drugs".

Note that the "4,000 offences" referred to in the Annual Report appears to be an error: an alternative figure of 13,964 offences was given in response to a Parliamentary Question in March 2006.[5] The Report (pages 31 and 32) explains that these estimates are based on a "retained acquittals" flag used to mark NDNAD records between May 2001, when the legislation allowing DNA records to be retained was adopted, and December 2005, when software for the Police National Computer (PNC) was modified to allow retention of the corresponding records on the PNC.

This is the most recent evidence available, covering the period to end March 2006, and is the source for the Prime Minister's claim.

All the sources cited make clear that the figures are based on estimates of the number of DNA profiles retained that would previously have had to be removed, followed by a further estimate of the number of matches that have occurred between these DNA profiles and DNA profiles obtained from biological samples (such as blood, hair, semen or saliva) collected at crime scenes.

2. What the Figures Mean

The figures cited by the Prime Minister are not based on the tracking of actual cases. Rather, they are based on a statistical estimate of the numbers of matches that may have occurred between crime scene DNA profiles and the DNA profiles of persons who were charged but not proceeded against or acquitted. This immediately introduces considerable uncertainty about how many matches have actually occurred, since the assumptions that have been made are not verifiable. Not only is the actual number of retained profiles from innocent people unknown, but it is unclear how the number of matches made with these profiles have been calculated, since the estimate does not correspond to specific individuals.

More importantly, the Prime Minister claimed in his speech that all these matches are with "*suspects*" and that these suspects "*would in all probability have got away*" had their DNA not been retained. However, DNA matches are not successful prosecutions and many matches occur with the DNA of individuals who are not the perpetrator of the crime, including victims and passers-by, or are false matches.

Only some matches, known as DNA detections, lead to someone being prosecuted for a crime, and not all DNA detections will lead to a conviction. The National Policing Agency (NPIA), which now runs the National DNA Database, states: "As convictions are achieved through integrated criminal investigation, not by forensic science alone, it is not possible to provide figures for the number of convictions produced by DNA".[6]

Roughly speaking, eight DNA matches lead to four detections, two of which lead to convictions, one of which will involve a custodial sentence.[7] However, only about half of these are "new detections, which require the Database—in the other cases the suspect will already have been identified prior to collection of their DNA. This means their DNA could be taken from them during the investigation and the existence of their record on

the Database is not necessary to obtain the match. These figures are dominated by volume crimes, such as burglaries, and separate figures are not available for more serious crimes such as rape and murder, for which the Database is less effective.

The Home Office notes that DNA has varying contributions to different types of crime and states in its report[3] (paragraph 50): "DNA has been shown to be of crucial importance in that subset of crimes where suspect identity is not immediately apparent, eg burglary and vehicle crime". Although DNA often provides important evidence in murder cases, it is extremely rare for a suspected murderer to be first identified via a "cold hit" on the Database: partly because murderers are often known to their victims and partly because it is often the victim's DNA (for example, in their blood found on the perpetrator's clothing) that is more useful in such cases. Similarly, although DNA evidence can be very important in some cases, most rapes involve disputes about consent (which cannot be resolved by taking DNA), not about identity.

Matches also include false matches, often because DNA profiles obtained from crime scenes are not complete. For example, the National DNA Database Annual Report 2005–06[4] (page 35) states that between May 2001 and April 2006, 50,434 matches with crime scene profiles, or 27.6% of the total number of match reports, involved a list of potential suspects, not a single suspect, being given to the police, because matches with multiple records on the NDNAD were made.

The Prime Minister's claim also fails to distinguish between the computerised DNA profiles held on the National DNA Database, and people's actual DNA (usually collected in a sample of their cheek cells taken at the police station using a mouth swab). The DNA samples are stored indefinitely by the commercial laboratories which analyse them for an annual fee, and raise additional privacy concerns because they contain unlimited genetic information. The retention of DNA samples has not contributed to the detection and prosecution of serious crime—only the retention of computerised DNA profiles on the NDNAD is necessary to obtain a match. The Home Office has recognised that retaining samples is "one of the most sensitive issues to the wider public"[8] and the Human Genetics Commission has concluded that the reasons given for retaining them are "not compelling".[9, 10]

3. Do the 114 Murderers Exist?

It is not possible—let alone probable—that 114 murderers would have walked away if DNA profiles from innocent people were not kept on the NDNAD, because the number of convictions is always considerably less than the number of DNA matches. In addition, suspects in murder cases are often identified by means other than a "cold hit" on the Database: claiming that they would "walk away" if they did not have a record on the Database is therefore highly misleading. Since the law changed, the Government has provided no examples of murders that have been solved as a result of retaining the DNA of innocent people beyond the period necessary to investigate whether they have committed a past offence.

The purpose of *retaining* an individual's DNA profile on a database (as opposed to collecting it) is to treat them as a suspect for any *future* crime. Although no figures are available, examples do exist of serious offenders whose DNA has been sampled in connection with a relatively minor offence and which has matched a past crime scene DNA profile when it is added to the Database. However, these cases are only relevant to discussion of when the police should be allowed to collect an individual's DNA, not whether they should keep it.

Brief details of two rape cases which do involve retention of DNA profiles from arrested persons have been provided in the National DNA Database Annual Report 2005–06 (page 14). These cases involve alleged violent disorder and assault, in circumstances where the victims have not been willing to press charges. In both cases the individuals went on to rape a stranger and to be identified by a match with their DNA profile held on the NDNAD. However, both cases raise more questions than they answer because of Britain's poor record in tackling rape and domestic violence.[11] It seems likely that these rapes could have been prevented by a more effective system to tackle violence against women at an earlier stage. A recent report by the Home Affairs Committee has concluded that the Government's approach to all forms of domestic violence remains disproportionately focused on criminal justice responses at the expense of effective prevention and early intervention.[12]

4. Just a Misunderstanding?

The Prime Minister's claim is not the first time that DNA matches have been confused with successful prosecutions, or that irrelevant cases have been cited in support of retaining innocent people's DNA.

4.1 *The debate in Scotland*

In 2005, the Scottish Executive held a public consultation on whether or not people who are arrested in Scotland should have their DNA retained following acquittal or if charges against them are not pursued.

On 14 February 2006, the Association of Chief Police Officers in Scotland's Lead on DNA Issues, the Chief Constable of Lothian and Borders police, claimed in the *Edinburgh News*[13]:

> "The most compelling argument for this change in law is that it will help us to catch criminals.
>
> This isn't some kind of theoretical forecast—we know from Home Office statistics that since 2001, when the law changed in England and Wales, police forces there have solved 10,000 offences using DNA that under the current law in Scotland would have to be destroyed.
>
> This includes 88 murders, 45 attempted murders, 116 rapes, 62 other sexual offences, 91 aggravated burglaries and 94 offences of the supply of controlled drugs".

As with the Prime Minister's more recent claim, this statement wrongly confused an estimate of DNA matches with actual solved crimes.[14]

GeneWatch UK published its first analysis of the UK Government's claims regarding the benefits of retaining DNA profiles from unconvicted persons in February 2006[7] and sent a copy of its report to Andy Burnham MP, then the Parliamentary Under Secretary of State at the Home Office with responsibility for the National DNA Database. In his reply of 15 March 2006, the minister stated:

> ". . . You raise important points about understanding the impact of DNA. The interpretation of statistics in the context of the processes which they represent is vital and **your analysis of that set of crimes for which DNA provided a first link to a suspect is sound**. These crimes are not the only ones in which DNA provides a useful contribution, however. Despite the apparent "losses" through the investigative process that you note, the presence of DNA can have additional benefits not represented in the statistics, such as reducing the time of the investigation, stopping criminals earlier in their careers and reducing subsequent court time". [Emphasis added]

In March 2006, the Justice 2 Committee of the Scottish Parliament sought further information regarding the benefits of DNA retention from unconvicted persons from the Association of Chief Police Officers in Scotland (ACPOS). They were provided with only one burglary case and two speculative murder cases, which had been solved but might have been solved more quickly had the individuals' DNA profiles been on the Database.[15]

The Scottish Parliament voted against indefinite retention of DNA profiles and samples from persons acquitted or not proceeded against, in May 2006.[16, 17] Instead, police powers were expanded to allow temporary retention (for up to 5 years, with judicial oversight) from a much smaller number of people who had been charged but acquitted of a serious violent or sexual offence.[18] The Scottish Government is currently conducting a review of this decision in order to assess whether the temporary retention of data from this more limited category of unconvicted persons is appropriate.[19] In conducting its review, the Scottish Government has expressly ruled out the indefinite retention of fingerprint and DNA data acquired from individuals who are not convicted of any crime. The Scottish Parliament reiterated its position in a vote on 28 February 2008, rejecting the blanket retention of DNA samples and fingerprints, and recognising that "appropriate utilisation of DNA samples and fingerprints can play an important role in identifying offenders but that it is vital to strike the right balance between prosecuting criminals and protecting the innocent".[20]

4.2 *The Marper case*

The Marper case—in which two innocent people are seeking removal of their DNA records[1]—was heard the the Grand Chamber of the European Court of Human Rights just days after the convictions of two killers in Britain as a result of DNA matches.

The convictions of Steve Wright, who murdered five women in Suffolk, and Mark Dixie, who killed Sally Anne Bowman, both highlighted the importance of DNA evidence. However, neither case would have been affected by a decision to remove innocent people's records from the Database.

Wright had a previous conviction for theft[21] and, even if his record had not been on the database, had already been stopped twice by the police before the crime scene DNA profile was obtained.[22] This means his DNA could have been taken by the police even if his record wasn't on the Database, although it would have taken longer before the match was made.

Sally Ann Bowman's killer Mark Dixie was not on the DNA Database, however he did have previous convictions which took place before the Database was established. The case was solved when his DNA was taken following a fight in a bar, nearly nine months after the murder. The police officer who headed the

investigation, Detective Superintendent Stuart Cundy, announced that the murder would have been solved much faster had there been a universal DNA database including everyone in Britain.[23] However, this neglected to discuss how Wright's DNA might have been included in this database. Adding adult volunteers onto the database would cost a lot of money and police time and be unlikely to catch any serious offenders, because they would simply not turn up to give their DNA. If DNA was taken at birth, in 10 years' time there would be a DNA database of every child under 10 who had been born in Britain—but this would not have helped to catch any murderers or rapists. The children on the database would be vulnerable to identification and abuse by anyone who could infiltrate the system.

The British Academy of Forensic Sciences has noted that "in reality there are a number of disadvantages" with profiling everyone at birth, which it lists as[24]:

- The scale of the operation would be disproportionate, since only a minority commit crimes.
- It would increase anxieties about "big brother", already evoked by widespread CCTV coverage and proposed biometric identity cards.
- It might be seen to imply that we are all guilty until proven innocent.
- There have, and will be, mistakes, chance matches and false matches with close relatives, made even more likely where profiles are incomplete.
- Links will be established all the time between the scene and innocent individuals, leading to false inferences.
- It would render every member of the population vulnerable to attack, by for example having their DNA planted at a crime scene.
- In future it is possible that profiles could also reveal confidential information about the health of an individual.
- It would be impossible to control for the large numbers of people who enter and leave the country, both legally and illegally.

The details of the Ipswich case, together with another case (the "RvB" case) were repeated in the European court, even though neither are relevant to the decision to retain DNA from innocent people. The "RvB" case involved an horrific rape, in which a match to an individual's DNA profile was made after his profile should have been removed, under the pre-2001 law. However, the details of the case show that the rape occurred before the individual's DNA was collected in connection with another crime (suspected burglary), and the problem only arose because his sample was not analysed for nearly nine months, until after his acquittal for the burglary.[25] New proceedures mean this should not happen again in the future.

5. Has Expanding the DNA Database Helped to Tackle Crime?

The NDNAD is a useful tool in criminal investigations, but the permanent retention on it of everyone who has been arrested for a recordable offence raises important concerns about privacy and rights, including:

- the potential threat to "genetic privacy" if information is revealed about health or family relationships, not just identity;
- the creation of a permanent "list of suspects" that could be misused by governments or others;
- the potential for unauthorised access, abuses and/or misuses and mistakes: including the tracking of individuals and their relatives, and the implications of false matches; and
- the exacerbation of discrimination in the criminal justice system.

GeneWatch UK is not opposed to the existence of the DNA Database, or the use of DNA in criminal investigations, but has questioned the benefits of its rapid expansion.

Overall, analysis of Home Office data shows that collecting more DNA from *crime scenes* has made a significant difference to the number of crimes detected using DNA, but keeping DNA from increasing numbers of individuals has not. In its 2006 report,[3] the Home Office states:

> "Evaluation of the [DNA Expansion] Programme has shown that the number of matches obtained from the Database (and the likelihood of identifying the person who committed the crime) is 'driven' primarily by the number of **crime scene** profiles loaded onto the Database" [emphasis added].

DNA detections increased significantly between 1998–99 and 2002–03, but the number of crime scene DNA profiles loaded onto the Database each year also more than tripled during this time (from 19,233 in 1998–99 to 65,649 in 2002–03[3]). Since 2002–03, the number of individuals with DNA profiles on the Database has doubled from 2 million to 4 million, but there has been no corresponding increase in the number of crimes

detected. DNA matches have gone down slightly and the chances of detecting a crime using DNA has remained roughly constant.

Year	*2002–03*	*2003–04*	*2004–05*	*2005–06*	*2006–07*
Number of individuals' DNA profiles stored†	2,099,964	2,371,120	2,802,849	3,534,956	3,976,090
Crime with DNA match	49,913	45,269	40,169	45,221	41,717
Crime with DNA detection*	21,098	20,489	19,873	20,349	19,949
Recorded crimes	5,920,156	6,042,991	5,623,263	5,556,513	5,428,273
Percentage of recorded crimes involving DNA detections	0.36	0.34	0.35	0.37	0.37

† These figures include some repeat records (an estimated 13.7% of the total). The 2006–07 figure is an estimated figure to 10 June, provided in response to a PQ. By October 2007, there were 4.1 million individuals with records on the NDNAD.

* House of Commons *Hansard* 30 April 2008 : Column 489W. The DNA database is only important for some of these DNA detections (about half), because for about half of them the suspect was already identified before being entered on the database.

Innocent people with records retained indefinitely on the NDNAD now include people who have been arrested for any recordable offence, aged 10 or above, who have not been charged, have had charges against them dropped or who have been acquitted.

By far the majority of these people have not had their DNA taken for the purposes of investigating the offence for which they have been arrested, because DNA is collected from less than 1% of crime scenes[26]: in general they will have no reason to have even been suspected of a serious crime such as rape or murder. It is therefore not surprising that the retention of their records (until age 100) on the Database has not increased the crime detection rate.

The Nuffield Council on Bioethics notes (paragraph 5.52)[27]:

> ". . . There is very limited evidence indeed that the retention regime of England and Wales is effective in significantly improving detection rates . . . The match rates between stored subject profiles and new crime scene profiles loaded onto the NDNAD in England and Wales, which is 52%, can be contrasted with that of the Scottish DNA Database, which has a higher match rate of 68%. This demonstrates clearly that the more limited retention policy in Scotland does not necessarily negatively impact upon its subsequent match rates".

Figures from the same report (paragraph 4.34) show that storing the DNA samples of the estimated 1 million innocent people on the DNA database costs about £1 million a year, resources that might be spent on alternative ways to tackle crime.

6. Conclusions

Examination of the evidence shows that:

- The figures cited by the Prime Minister refer to an estimate of DNA matches, not solved crimes.
- The reported matches are not actual matches obtained with individuals' profiles retained on the NDNAD following acquittal or charges being dropped, but are an estimate based on a number of unverifiable assumptions.
- DNA matches are not successful prosecutions and many matches occur with the DNA of individuals who are not the perpetrator of the crime, including victims and passers-by, or are false matches.
- The retention of DNA samples has not contributed to the detection and prosecution of serious crime—only the retention of computerised DNA profiles on the NDNAD is necessary to obtain a match. The DNA samples are stored by the commercial laboratories which analyse them for an annual fee, and raise additional privacy concerns because they contain unlimited genetic information.
- Misinformation about the impact of DNA retention on solved crimes is likely to mislead the public about the recent massive expansion of the National DNA Database. Retaining innocent individuals' DNA is costly but has delivered no detectable improvement in solving crimes: this contrasts with the improved collection and analysis of crime scene DNA.

GeneWatch UK concludes that:

1. The Prime Minister's claim that "in all probability" 114 murderers would have walked away had innocent people's records not been retained on the National DNA Database is false.
2. Ministers are well aware that this claim is false.
3. This figure is seriously misleading to members of the public who are concerned about the implications of retaining innocent people's records indefinitely on the National DNA Database.

References

[1] This case was subject to an appeal to the European Court of Human Rights, from which a judgment is awaited. The two applicants, Marper and "S" (a juvenile) are seeking removal of their records and destruction of their DNA, following cases in which charges were dropped and the individual was acquitted, respectively.

[2] House of Lords (2004). http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040722/york-1.htm

[3] Home Office (2006) DNA Expansion Programme 2000–05: Reporting achievement. Forensic Science and Pathology Unit. http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/DNAExpansion.pdf

[4] *The National DNA Database Annual Report 2005–06*. http://www.homeoffice.gov.uk/documents/DNA-report2005-06.pdf

[5] House of Commons *Hansard* 1 March 2006 : Column 842W.

[6] Neyroud P (2008) Letter to Tom Levitt MP, Re: Letter from Helen Wallace. 25 April 2008.

[7] GeneWatch UK (2006) The DNA expansion programme: reporting real achievement? February 2006. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAexpansion_brief_final.pdf.

[8] Home Office (2005). Supplementary Memorandum, Appendix 20. In: House of Commons Science and Technology Committee (2005) Forensic science on trial, Volume II. HC 96-II, www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96ii.pdf.

[9] Human Genetics Commission (2002), *Inside information*, May 2002. http://www.hgc.gov.uk/UploadDocs/DocPub/Document/insideinformation_summary.pdf.

[10] Human Genetics Commission (2005) HGC response to the Scottish Executive consultation on police retention of prints and samples, http://www.scotland.gov.uk/Resource/Doc/77843/0018244.pdf.

[11] End Violence Against Women (2007) *Making the grade?* 2007. The third annual independent analysis of UK Government initiatives on violence against women. http://www.endviolenceagainstwomen.org.uk/data/files/evaw_mtg_uk.pdf

[12] Home Affairs Committee (2008) Domestic violence, forced marriage and "honour"-based violence. Sixth Report of Session 2007/08. Vol I. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/263/263i.pdf

[13] Tomkins P (2006) Clear evidence for switch in DNA law, *Edinburgh News*, 14 February 2006. http://edinburghnews.scotsman.com/comment/Clear-evidence-for-switch-in.2750809.jp

[14] Morgan J (2006) Police DNA records plan "fails to solve more crimes" Warning on keeping profiles of the innocent, *The Herald*, 27 February 2006.

[15] ACPOS(2006) Letter from Chief Constable William Rae to Mr Steven Talloch, Justice 2 Committee. 24 March 2006.

[16] Scottish Parliament Justice 2 Committee Official Report 28 March 2006. http://www.scottish.parliament.uk/business/committees/justice2/or-06/j206-0902.htm#Col2146

[17] Scottish Parliament Official Report, Police, Public Order and Criminal Justice (Scotland) Bill: Stage 3. 25 May 2006. http://www.scottish.parliament.uk/business/officialReports/meetingsParliament/or-06/sor0525-01.htm.

[18] http://www.scotland.gov.uk/News/Releases/2007/01/29133555.

[19] Scottish Government Review, 3 December 2007.

[20] http://www.scottish.parliament.uk/business/chamber/mop-08/mop08-02-28.htm.

[21] Ipswich accused: "Yes I used prostitutes", Sky News, 7 February 2006. http://news.sky.com/skynews/article/0,,30100-1304402,00.html.

[22] Fresco A (2008) Scientists' elation at finding DNA that led to a murderer, *The Times*, 22 February 2008. http://www.timesonline.co.uk/tol/news/uk/crime/article3410814.ece

[23] Kelly J (2008) DNA database debate urged, BBC Online, http://news.bbc.co.uk/1/hi/uk/7259494.stm

[24] British Academy of Forensic Sciences (2007) Submission to the consultation held by the Nuffield Council on Bioethics on "The forensic use of bioinformation: ethical issues". http://www.nuffieldbioethics.org/fileLibrary/pdf/British_Academy_of_Forensic_Sciences.pdf

[25] Williams R, Johnson P, Martin P (2004) Genetic information and crime investigation. p 36.

[26] In 2004–05, 913,717 crime scenes were examined (16.2% of crime scenes), potential DNA material was collected from 12% of these, and 45% of these crimes yielded DNA profiles that were uploaded to the Database. Paragraphs 23–25, Home Office (2006).

[27] Nuffield Council on Bioethics Report: The forensic use of bioinformation: ethical issues. http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/introduction.

June 2006

WEDNESDAY 6 FEBRUARY 2008

Present	Bledisloe, V	O'Cathain, B
	Goodlad, L (Chairman)	Peston, L
	Lyell of Markyate, L	Rodgers of Quarry Bank, L
	Morris of Aberavon L	Rowlands, L
	Norton of Louth L	

Memorandum by Liberty

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at:

http://www.liberty-human-rights.org.uk/publications/1-policy-papers/index.shtml

Introduction

1. Liberty is delighted that the House of Lords Constitution Committee is undertaking an inquiry into the impact of surveillance and data collection upon the privacy of citizens and their relationship with the state. Surveillance and data collection raise profound ethical and constitutional issues and Government schemes like the DNA Database and ID Cards have the potential to change the nature of the relationship between state and citizen. Parliament is particularly well-placed to assess the wider societal impact of measures which interfere with personal privacy. While the courts, for example, often focus on individual cases, Parliament is better able to look at the broader picture. This is particularly important in this context. Policies like the permanent retention of DNA on the DNA Database involve less tangible human rights infringements than measures which, for example, deny people a fair trial. It is only when one aggregates the impact of such measures across the millions of people they affect that one can see the real extent of their effect on privacy and their significant constitutional implications.

A Human Rights Approach to Privacy

2. Liberty starts from the position that privacy matters. If in any doubt about this you need only ask whether you would be happy to have a CCTV camera in your living room, whether you draw the curtains before you change for bed or whether you would be upset to discover that the police have been listening in to your telephone calls. It is not only those that have something to hide that have something to fear, something to protect. The post-War human rights framework recognizes the importance of personal privacy to human dignity and to peoples' ability to live their own lives and develop their own personalities and relationships. The concern of modern human rights instruments with privacy is also closely connected to the world's experience of abusive, totalitarian regimes. A near-complete denial of private life was a clear result of fascism and shown to be a great human cost. Complete disrespect for private life was also vital to the maintenance of power by dictatorial regimes, a chillingly effective tool of oppression. It was not only that the work of secret police deterred opposition, though certainly it did. Undermining personal privacy also undermined personal

resistance, the ability of many people to maintain a concept of themselves as individuals, divisible and perhaps opposed to the regime:

> "No, retiring into private life was not an option, However far one retreated, everywhere one was confronted with the very thing one had been fleeing from. I discovered that the Nazi revolution had abolished the old distinction between politics and private life, and that it was quite impossible to treat it merely as a 'political event'. It took place not only in the sphere of politics, but also in each individual private life; it seeped through the walls like poison gas."[1]

3. This is not, however, to say that all Governments that infringe personal privacy are dictatorial or fascistic. Liberty neither likens Tony Blair to Hitler and Stalin nor the British police to the Stasi. We do, however, believe that the lessons the world learnt about the importance of privacy during the 20th Century remain vital tools today for understanding and scrutinising Government proposals and for protecting personal privacy against unjustified or arbitrary interferences. Like most rights in the post-War human rights framework, the right to personal privacy is not absolute. It recognizes that surveillance is sometimes justified and that it is sometimes necessary for the state to take, share and use personal information. A human rights approach to personal privacy does, however, require a few basic questions to be asked before the latest policy, technology or investigative technique is given the go ahead: (1) Is there legal authority for the privacy infringement in question?; (2) Is there a legitimate reason for the intrusion of privacy?; and (3) Could that legitimate aim be achieved in a way which does not intrude into a person's privacy or could do so less? It also reminds us to be diligent about measures which have an arbitrary or discriminatory impact on certain social groups. These basic, common sense questions are, we believe, integral to good policy-making, Government accountability, an engaged citizenship and a healthy democracy.

A Surveillance State—Overview

4. In November 2006 the Information Commissioner Richard Thomas said "Two years ago I warned that we were in danger of sleepwalking into a surveillance society. Today I fear that we are in fact waking up to a surveillance society that is already all around us." His words came at the time "A Report on the Surveillance Society"[2] was published. Liberty agrees with the assessment made by the Information Commissioner. Like him we also accept that surveillance is an unavoidable and often justified aspect of life in the early 21st century. However, the extent to which every person in the UK is subjected to surveillance has increased disproportionately to any justifying social need or benefit.

5. "Surveillance" can usefully be sub-divided into different types:

- "Mass informational surveillance" relates to the retention and dissemination of database information. This would cover databases such as the National Identity Register (NIR), created by the Identity Card Act 2006 (IDCA) and the Children's Index set up by the Children Act 2004.
- "Mass Visual Surveillance" relates to the use of CCTV cameras.
- "Targeted Surveillance" refers to the use of intrusive powers such as communication interception by means of the framework created under the Regulation of Investigatory Powers Act 2000 (RIPA).
- Finally, the retention of DNA retained on the National DNA Database (NDNAD) is arguably surveillance.[3]

The central distinction between these types of surveillance is that targeted surveillance is commonly used as part of an intelligence-led investigation into illegal or unlawful activity. Mass visual and informational surveillance does not take place in anticipation of a specific investigation into impropriety but will often be claimed to have some crime detection or (in the case of CCTV) crime prevention purpose. Information is retained and disseminated in anticipation of being of use for investigation. Mass informational surveillance will also take place for purposes unrelated to investigation such as assisting access to public services.

6. Mass and targeted surveillance techniques have usually been distinct. However, in the last few years this distinction has been blurred by increasing use of "data matching" and "data mining" processes. These techniques are based on the use of automated processes which analyse or match seemingly innocuous data in order to throw up anomalies or inconsistencies. When used in relation to information about people this is more commonly known as "profiling". The blurring of distinction arises from the fact that there is no human or intelligence led initiation of suspicion. Human investigation will follow after initial matching or mining.

[1] Sebastian Haffner, *Defying Hitler: a memoir*, (London, 2003), p.180
[2] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf
[3] It is, however, distinct from mass informational surveillance in that it is "data" that (at present) serves a specific single purpose which cannot be applied elsewhere.

7. In this short response we will make brief observations on all these forms of surveillance along with appropriate conclusions and recommendations. Liberty will be publishing a substantive work on surveillance and privacy over the summer which will cover in far greater detail some of the issues touched on here.

Mass Informational Surveillance

8. Proliferation of CCTV might attract more observation and comment but the increase in informational database use has arguably been the more profound societal shift in the last decade. Access to and use of mass informational databases is part and parcel of everyday life, whether it is almost instant information provision via an internet search engine or identifying a postal address by way of a postcode and house number. Mass informational database use is increasingly being used as a tool of government though programmes such as the compulsory NIR or the Children's Index.[4]

9. Liberty's views on the undesirability and likely ineffectiveness of the NIR are well documented and we do not intend to repeat these here. There are, however, several points that can be made about the IDCA that are relevant to consideration of the surveillance society. The reserved powers scattered throughout the Act allow scope for the range of uses and purposes of the NIR, and those who can have access to it, to be increased. If the NIR comes into existence then it is likely to make logistical, financial and political sense to increase the purposes it serves. If, for example, the NIR had been in operation at the time of Ian Huntley's conviction for the Soham murders, the mood of public outrage was such that there would have been political pressure to place details of convictions or "soft" non-conviction police intelligence onto NIR entries[5]. The experience of the previous World War II identity cards suggests that extra purposes would be found as that scheme saw an increase in uses from three to 39 in 11 years. A further point worth making is that as the identity cards scheme is rolled out, the NIR will also allow a detailed audit trail of individual activities to be drawn on each entry by virtue of the entries permitted by paragraph 9 of Schedule 1 IDCA. If private sector agencies such as banks gain access to NIR as a means of verifying identification, the detail on this audit trial will increase.

10. Liberty does not believe that there is any justification for the NIR but does not take this position in relation to others mass informational databases. For example, we accept that the Children's Index was created to protect children—clearly a legitimate purpose. We did, however, take issue with the Bill when it was passing though Parliament. The policy driver for information sharing powers was the tragic death of Victoria Climbié. The implication was that social workers in her case were somehow prevented from sharing information. In reality information sharing powers were available. Victoria's death was more a result of a catalogue of mistakes and the fact that those responsible for her care lacked training, resources and guidance. Liberty also felt that the proposals were so broad and poorly framed as to raise significant concerns over the privacy of children and families. We believed the Index might in practice undermine child protection. So much information would be gathered that children genuinely at risk might be overlooked as a consequence of "not seeing the woods for the trees". However, we do believe that the Children's Index, if limited in scope and effectively regulated, could prove to have genuine child protection benefits. The application of Human Rights principles of necessity, proportionality and legitimate purpose could ensure that only appropriate information is entered into the Index and only those who have proper justification would have access. Effective oversight of the ICO would also be essential for proper operation. As previously stated, there is not the space to provide more detail in this document.

11. Liberty's forthcoming work on privacy gives more detail on this subject. However, the example of the Children's Index encapsulates Liberty's approach to mass informational surveillance. Used effectively, it can be of public benefit. Used excessively, it infringes privacy and can be counterproductive. Human rights principles and effective regulation can provide a framework for striking a balance. Unfortunately, comments made by the Prime Minister earlier this year indicate that the prevailing attitude in government is that mass public sector information sharing is, by its nature, desirable.

Mass Visual Surveillance

12. The proliferation of CCTV in the UK is well documented. Hardly a week passes without new newspaper reports of advances in CCTV technology. Most recently headlines have focused on talking CCTV: "Big Brother is Shouting at You" (*Daily Mail*, 16 September 2006), "Oi! Talking CCTV cameras will shame offenders" (*Daily Telegraph*, 6 April 2007), "Talking CCTV gives Big Brother a voice" (*Daily Telegraph*, 5 April 2007), "Oy! Big Brother is talking to you" (*Sunday Times*, 4 March 2007). Liberty believes that CCTV has some limited crime detection use but negligible crime prevention use. At most, it can play a part in a holistic

[4] The Children's Index is intended to assist child protection by allowing different services the ability to enter and access details of children onto the index, including anything that might constitute a "cause for concern" (discussed below).

[5] As it was the Bichard Inquiry into the killings made the commendable suggestion that a positive vetting process be introduced.

approach to combating crime. Whether new generation systems will prove to be of greater use in combating crime than their predecessors remains unproven. Many improvements seem little more than gimmicks.

13. Liberty has two principal areas of concern over the use of CCTV. First, it remains effectively unregulated. The legislation that can, but often does not, apply to CCTV is the Data Protection Act 1998 (DPA). However the DPA is not intended to provide a comprehensive framework for CCTV regulation. The data protection principles in the DPA cater for the processing, retention and dissemination of data. They do not provide any detail on, for example, the need to justify the location of cameras, notification of location, good practice on handling footage and so on. Good guidance does exist for the use of both private and public sector systems but these are effectively voluntary and unenforceable.[6]

14. Our second principal concern is that even the limited applicability of the DPA only relates to a small number of CCTV cameras. The case of *Durant* in 2004 resulted in many systems not being subject to the DPA at all.[7] The basic position is that CCTV is only covered by the DPA if it can be shown that a system is targeted on an identifiable subject. Clearly many systems, especially those set up by public authorities, do not target individuals and would not be governed by the DPA. As a consequence, CCTV in the UK remains largely unregulated.

15. In March 2007 the Council of Europe Venice Commission published an opinion on video surveillance in public places and the protection of Human Rights[8]. It laid out the Venice Commission's views on the data protection and human rights requirements of legislation and good practice governing the use of CCTV. Its conclusions serve as a useful reminder of the societal impact of CCTV upon a country where it has become ubiquitous:

> "Video surveillance of public areas by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy … and his/her right to benefit from specific protection regarding personal data collected by such surveillance … it is recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy."[9]

Intrusive Surveillance

16. The use of intrusive surveillance is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). The call for evidence does not mention RIPA. However, given that the most invasive surveillance uses RIPA powers, we will make a few observations. There can be no argument against the proportionate use of surveillance powers by the state particularly when involving investigations into serious crime and threats to national security.

17. The use of RIPA has increased considerably since it was passed. To an extent, this might be justified by increased concerns over national security. However the sheer scale of RIPA use is staggering. In February 2007 the Interception of Communication Commissioner, Sir Swinton Thomas, reported that over 439,000 requests for communications traffic data were made in the period 1 January 2005 to 31 March 2006[10]. A total of 2,243 intercept warrants were issued in the same 15 month period[11].

18. The scale of surveillance can be attributed to several factors. The scope of those able to use RIPA powers is wide with a huge range of public bodies having access to them. RIPA orders published as secondary legislation set out those bodies with access to RIPA powers. However, they receive scant Parliamentary time and are, in any event, unamendable. RIPA powers are often self-authorising with lower level communications data powers being authorised internally and even the highest level interception powers only requiring the authority of a government minister. This can be contrasted with the USA where, historically, there has always been independent judicial authorisation at the heart of the US surveillance process. Any surveillance warrant against a US citizen needs to be granted by a court. Meanwhile, interceptions of Communications to the US

[6] See for example the guidance issued by the Information Commissioners Office in 2000 for operators of CCTV systems http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf and *"A Watching Brief—A Code of Practice for CCTV"* aimed at public sector users of systems published by the Local Government Information Unit in 1996

[7] *Durant v Financial Services Authority* [2004] F.S.R 28, CA

[8] http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

[9] Ibid paragraphs 79–81

[10] "Communications data" are records (but not the contents) of communication traffic such as mobile phone calls and email records. According to the report for 2005–06 there were 439,054 requests http://www.ipt-uk.com/docs/HC315.pdf

[11] "Intercept warrants" allow interception of communications so that the contents of communications can be recorded

originating from overseas need authorisation from a special Foreign Intelligence Surveillance Court. After the September 11th bombings, attempts by President Bush to introduce a limited scheme of executive authorisation of warrants (ie similar to the UK's) were deemed unconstitutional by the US Federal Court.[12]

The National DNA Database (NDNAD)

19. The UK retains five times as many of its population on the NDNAD as any other country. In recent years the grounds for taking and permanently retaining DNA has expanded from those who are convicted of offences, to the current position of retention on arrest for any recordable offence. There is discretion for the police to remove a sample but this seems only to be exercised in exceptional circumstances. There are indications that the grounds for retention may soon be increased again to cover arrest for non-recordable offences[13].

20. Liberty believes that the continued rolling out of the database will eventually result in a "tipping point", whereby a large enough proportion of the population are on the register to justify the case for compulsory entry for all on the NDNAD. We believe that if this is the intention then the case for compulsory retention should be made now. Liberty accepts that there is a need for a limited database of those convicted of certain offences (generally involving violence or sexual assault). However DNA is irrelevant in most criminal cases and the vast majority of entries on the register will be of no use in solving crimes.

21. It is very difficult to have a debate on the NDNAD as discussion usually takes place following the DNA assisted conviction of a person for a gruesome historical crime. It is difficult to weigh the "light effect, wide impact"[14] effect of DNA retention on the population as a whole in the context of this type of case. Again there is not space here to discuss these issues in detail but it is worth noting that the impact of roll out has had a hugely disproportionate impact upon certain demographics, particularly Afro Caribbean males. It has also resulted in the permanent retention of thousands of young people under 16 with no criminal conviction or caution. Balanced against this is an admission from the Government that there is no evidence that taking the DNA from those who have not been convicted has helped crime detection.[15] Furthermore, although there has been a massive extension of the NDNAD over the last three to four years, the rate of crime detection using the Database has stayed at about 0.35% of all recorded crime. If extending the size of the NDNAD had been successful one would expect this proportion to have increased.

Data Matching, Data Mining and Profiling

22. As mentioned in the introduction, data mining and data matching techniques are increasingly being used for crime detention. A recent Home Office White Paper gave details of plans to increase the use of data mining techniques.[16] The Serious Crime Bill before Parliament formalises data matching practices in relation to fraud. These practices are a consequence of increased technological sophistication coupled with vast quantities of data held on mass informational databases, making traditional human led intelligence policing more difficult.

23. As well as raising significant issues of proportionality and legitimate purpose, there are several specific points that the Committee might consider. Of particular significance and central to Liberty's analysis of the surveillance society is that data matching and data mining practices have outstripped data protection legislation. The DPA is nearly 10 years old. The European directive, upon which the DPA is based, dates from 1995.[17] The regime created by the Act and its accompanying principles might have provided an adequate framework at a time when "processing" more usually involved the processing of small amounts of data. However, the DPA is not equipped to cope with mass data processing exercises. For example, the second data protection directive permits data processing only for one or more specified purposes. However, all that is required is for these purposes to be notified to the Information Commissioners Office (ICO). This would allow mass processing for multiple purposes provided that the ICO is notified. Notification is essentially an

[12] *American Civil Liberties Union et al., v. National Security Agency / Central et al.*, United States District Court for the Eastern District of Michigan, 17 August 2006

[13] See the recent Home Office consultation "Modernising Police Powers: Review of the police and Criminal Evidence Act" (PACE) 1984 at paragraph 3.33 "The absence of the ability to take fingerprints etc in relation to all offences may be considered to undermine the value and purpose of having the ability to confirm or disprove identification and, importantly, to make checks on a searchable database aimed at detecting existing and future offending and protecting the public. There have been notable successes particularly through the use of the DNA database in bringing offenders to justice". http://www.homeoffice.gov.uk/documents/cons-2007-pace-review?view=Binary

[14] "Light impact, wide effect" measures are ones which have a relatively small impact upon an individual but which have a considerable cumulative effect upon society.

[15] Home Office Minister Joan Ryan 9 October 2006 "As far as we are aware, there is no definitive data available on whether persons arrested but not proceeded against are more likely to offend than the population at large." HC Deb, Col 491W

[16] New Powers Against Organised and Financial Crime

[17] Directive 95/46/EC

administrative matter. The ICO has no ability to refuse notification and what limited enforcement powers exist, can apply only once processing has already taken place.

24. As mentioned earlier, data matching and mining processes applied to people can be called profiling. Following the terrorist bombings in July 2005 and the alleged aeroplane hijackings in August 2006, there were calls from a variety of sources to adopt profiling on public transport and for flight passengers. So far, we are pleased to see that there have been no moves in this direction. However, we are concerned that the growth of mass informational databases might make moves towards profiling difficult to resist. The National Identity Register is a good example of how this might occur. After the July 2005 attacks, the former Home Secretary, Charles Clarke, publicly accepted that ID cards and the NIR would not have prevented the attacks. This makes sense as it is safe to assume that British intelligence and policing agencies have gathered information on anyone that they believe could constitute a risk to national security. The reality is that anyone who does give reason for concern would become subject to a level of targeted surveillance that would collate information going way beyond what would be contained on the NIR. It is not feasible that the NIR entry would add to that possessed by the Security Services. This leads to a worrying possibility: in order to be of any use whatsoever in combating terrorism, the NIR must contain more information. This would need to be of a type that would separate those who present no, or minimal, risk to national security from those who might pose a serious risk. In other words, to be of any use in combating terrorism, data contained on the NIR must be increased in order to allow some degree of profiling and categorisation.

Conclusion

25. Space considerations preclude anything other than a brief summary of the steps Liberty believes are appropriate to protect privacy against unwarranted surveillance. If the Committee is taking oral evidence we would welcome the opportunity to discuss our observations and conclusions in greater detail. Liberty believes that the legislative and regulatory framework has failed to keep place with surveillance. As explained above, the DPA is out of date. New data protection legislation is needed to reflect changes in data processing techniques and to properly regulate CCTV. The ICO needs better resources and more proactive powers to properly police surveillance. The ICO should also be heavily involved in the drawing up of guidance and good practice in information access and dissemination.

26. The role of Parliament also needs to be enhanced by ensuring individual Commissioner's report to Parliament rather than to ministers.[18] As details of information access and sharing are typically reserved for secondary legislation, Parliament should be more readily given the power to amend regulations.[19] Privacy impact statements should be introduced to accompany Bills. More independent judicial authorisation of interception powers under RIPA are necessary, as is greater oversight and control of communications data access. There should be no further roll out of DNA retention powers and a presumption in favour of sample destruction should be introduced for those not charged or convicted. These measures will re-introduce proportionality and accountability to surveillance. They require political will but would help counter growing public unease about the extent of the surveillance society.

June 2007

Memorandum by JUSTICE

Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is the British section of the International Commission of Jurists.

2. JUSTICE welcomes the Committee's inquiry into the impact of surveillance and data collection upon privacy and the relationship between citizens and the State. Although we recognise that surveillance and data collection can sometimes be a legitimate tool (eg in the fight against crime)—few would dispute the usefulness of such developments as search engines and databases—but such advances also have an obvious potential to interfere with individual privacy if not properly regulated. In particular, they place an unprecedented amount of personal information in the hands of the state. However benign the state's intent, the potential for misuse is vast.

[18] The Interception of Communication Commissioner, The Surveillance Commissioner and the National Identity Scheme Commissioner
[19] As has happened in the ID card act in relation to information that can be recorded in the NIR

3. JUSTICE has long been concerned with the impact of various kinds of surveillance[20] and data-collection—from the increasing use of public and private databases to the growth of CCTV—on the protection of privacy as a fundamental right. For instance, we first pressed for data protection controls in our 1970 report, *Privacy and the Law*. In 1998, we published *Under Surveillance: Covert policing and human rights standards*, arguing for much closer regulation of governmental powers in this area.

4. Sadly, the development of effective legal and practical safeguards for individual privacy have lagged far behind the pace of technological developments and the uptake of surveillance technologies by both the public and private sector. Indeed, as a number of recent reports have shown,[21] the UK has the dubious reputation as a market leader among western nations in a number of surveillance-related fields, from the scale of the national DNA database ("NDNAD"), the number of CCTV cameras per capita, to the adoption of biometrics in passports and drivers licences. Due to constraints of space, however, this submission is not meant to provide a comprehensive analysis but instead, it deals only with the broader human rights issues arising from surveillance and data-collection.

Privacy as a Public Good

5. In the debate over surveillance, it is often assumed that the interests at stake are those of the general public versus the individual's interest in maintaining his or her privacy. We think such a view is both simplistic and mistaken, relying on a false opposition between the public interest and the individual right to privacy.

6. In our view, privacy is best understood as a public good. By this we mean that there is a collective interest in maintaining a society in which personal privacy is protected. There are a number of reasons for this, not the least of which is that a free society is one that respects individual freedom to live a life without undue interference or scrutiny. Another reason is the belief that individuals are more likely to be contribute to the maintenance of a good society where they recognise that that society is concerned to protect their own rights, including the right to privacy.

7. The maintenance of privacy as a collective good, however, requires not only governmental action but also restraint. In our view, threats to privacy are likely to come as much from unnecessary and over-intrusive governmental measures, such as the Identity Cards Act 2006, as from surveillance or data-gathering by the private sector. Too often, the government's enthusiasm for the administrative or forensic benefits of new technologies appears to outstrip its respect for privacy. The importance of restraint by government is particularly important in the context of the UK's common law tradition.

Privacy and the Common Law Tradition

8. Unlike the overwhelming majority of European jurisdictions,[22] the UK is a common law jurisdiction. The way in which privacy is protected under UK law therefore differs significantly from the way in which it is protected in continental legal systems, notwithstanding the overarching protection provided by the right to respect for private life under Article 8 of the European Convention on Human Rights ("ECHR"). In particular, because the conventional approach of the common law is one of "negative liberty" (ie whatever is not prohibited by statute is permitted),[23] privacy was traditionally protected by the absence of legislation

[20] By "surveillance", we mean not only "directed" or "intrusive" surveillance as defined in subsections 26(2) and (3) of the Regulation of Investigatory Powers Act 2000 (ie covert surveillance by law enforcement or intelligence bodies likely to obtain private information about an individual, including private residences), but also what might be termed "passive" or "undirected" surveillance, eg information gathered by a CCTV camera. Whether it is analytically helpful to describe large-scale practices of data-gathering, retention, sharing, mining and profiling as "surveillance" per se is something we do not address. But the practices of data-mining etc have an obvious common factor with surveillance: the use of personal data for the purpose of monitoring, policing or regulating individual conduct. Given that data gathered for one purpose (eg health care) may readily be used for another (eg investigating criminal activity), it makes sense to consider the general establishment of databases by the public and private sector as an aspect of the surveillance debate.

[21] See eg Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007); Surveillance Studies Network, *A Report on the Surveillance Society* (September 2006).

[22] The only other EU member state with a common law system is the Republic of Ireland. However, the right to privacy is there recognised as an unenumerated constitutional right implied within the scope Article 40.3 of the 1937 Constitution: see eg the Supreme Court decision in *Kennedy v Ireland* (1987) IR 587 per Hamilton P: "Though not specifically guaranteed by the Constitution, *the right to privacy is one of the fundamental personal rights of the citizen* which flow from the Christian and democratic nature of the State. It is not an unqualified right. Its exercise may be restricted by the constitutional rights of others, or by the requirements of the common good, and it is subject to the requirements of public order and morality . . . The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society" [emphasis added].

[23] See eg Lord Steyn, "Democracy, the Rule of Law and the Role of Judges", Attlee Foundation Lecture, 11 April 2006: "The spirit of liberty is the dominant theme of the common law. Whatever is not specifically forbidden, individuals and their enterprises are free to do. By contrast the government and its agencies may only do what the law permits; what is done in the name of the people requires constant examination and justification".

rather than a specific set of legal principles.[24] It was therefore unnecessary for the common law to develop such principles.

9. Even with the growth of new technologies and governmental measures impinging on privacy, however, the courts have remained reluctant to develop a common law right of privacy, primarily because of a concern that it would involve regulation of a kind far more detailed than common law rules are normally able to achieve and, indeed, far beyond the democratic competence of the courts to provide.[25] The data protection principles in Schedule 1 of the Data Protection Act 1998 ("DPA"), for example, would have been well outside the institutional capability of the courts to develop.

10. For this reason, the common law right to privacy has remained significantly underdeveloped, by contrast with most European jurisdictions and, indeed, even by comparison with many other common law jurisdictions.[26] Although section 6 of the Human Rights Act 1998 imposes a positive duty on public authorities to act compatibly with Convention rights—including Article 8 ECHR—it is important to bear in mind the limitations of Article 8. As a qualified right, it affords significant leeway to national authorities to interfere with personal privacy for various governmental purposes.[27] Nor is the European Court of Human Rights in a position to develop a UK law of privacy in the absence of action by the UK courts and Parliament. Most of all, the protection to privacy afforded by Article 8 should be seen as "a floor, not a ceiling".[28] Although we regard the Human Rights Act 1998 as a constitutional document and the rights protected therein as constitutional rights,[29] it is also important to bear in mind the limitations of the legal framework for protection of constitutional rights in the UK.

11. Also, while we welcome the influence of comparative law, particularly in terms of understanding the UK's obligations under the ECHR and EU law, we are concerned at the government's reliance on examples of European practice in debates on privacy measures, eg the widespread use of ID cards in many continental jurisdictions. In our view, it is unhelpful to cite the experience of European jurisdictions on such matters without having regard to the wholly different sets of checks and balances that exist in those jurisdictions to protect personal privacy. Given the widespread lack of understanding of the differences between the common law and continental legal systems, such examples can only have a deeply misleading impression.

12. Ultimately, while Article 8 ECHR and section 6 of the Human Rights Act provide an important check against arbitrary and intrusive measures, it is a mistake to suppose that judicial supervision is enough to maintain privacy as a public good in the UK. In particular, Parliament cannot abdicate to the courts its responsibility to govern well, in particular by restraining the executive's enthusiasm for the administrative benefits of surveillance and data-collection.

[24] As Lord Hoffman noted in *Wainwright v Secretary of State for the Home Department* (2004) 2 AC 406 at para 31: "There seems to me a great difference between identifying privacy as a value which underlies the existence of a rule of law (and may point the direction in which the law should develop) and privacy as a principle of law in itself. The English common law is familiar with the notion of *underlying values*—principles only in the broadest sense—which direct its development. A famous example is *Derbyshire County Council v Times Newspapers Ltd* [1993] AC 534, in which freedom of speech was the underlying value which supported the decision to lay down the specific rule that a local authority could not sue for libel. But no one has suggested that freedom of speech is in itself a *legal principle* which is capable of sufficient definition to enable one to deduce specific rules to be applied in concrete cases. That is not the way the common law works" [emphasis added].

[25] See eg *Malone v Metropolitan Police Commissioner*, [1979] 2 All ER 629 per Megarry VC at 649: "telephone tapping is a subject which cries out for legislation"; Lord Hoffman in *Wainwright*, n5 above, para 33: "[the creation of a tort of invasion of privacy] is an area which requires a detailed approach which can be achieved only by legislation rather than the broad brush of common law principle".

[26] The more developed right to privacy in some other common law jurisdictions can be attributed to the greater constitutional role accorded to the courts in those jurisdictions in protecting fundamental rights, see eg the development of the right to privacy by the US Supreme Court in *Roe v Wade* 410 U.S. 113 (1973).

[27] See Article 8(2): "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". As the European Court of Human Rights noted in *Peck v United Kingdom* (2003) 36 EHRR 41 at para 77: "In cases concerning the disclosure of personal data, the Court has also recognised that a margin of appreciation should be left to the competent national authorities in striking a fair balance between the relevant conflicting public and private interests".

[28] Labour Party Manifesto 1997: "The incorporation of the European Convention will establish a floor, not a ceiling, for human rights". See also eg Lord Woolf, "Human Rights and Minorities", 13 April 2003: "It is acknowledged that the introduction of the [ECHR] in domestic law provides a 'floor not a ceiling' for the protection of human rights. It is of crucial importance that we continue to build upwards"; Feldman, "The Impact of the Human Rights Act on English Public Law", British Institute for International and Comparative Law, 7 October 2005: "We also know that the [ECHR] and the transformation of the Convention rights into municipal law are intended to operate as a floor, not a ceiling: authorities are free to adopt a higher standard of human rights protection than that required by the Strasbourg court so long as they do not fall below the Strasbourg standard".

[29] See eg Lord Steyn, "Democracy, Rule of Law and the Role of Judges" Attlee Lecture, 11 April 2006, "The second premise of the democratic idea is that the basic values of liberty and justice for all and respect for human rights and fundamental freedoms are guaranteed. It is enshrined in the Human Rights Act 1998 which is our Bill of Rights".

The Need for Governmental Restraint

13. In our view, the government typically fails to address in a principled manner the core elements of the right to privacy under Article 8 ECHR: (i) whether a particular measure that interferes with personal privacy is necessary; and, if so, (ii) whether the interference is proportionate to the particular aim that the government seeks to pursue. In short, the government frequently seems more concerned with whether it could establish a new database, etc, and not with the more important question of whether it should.

14. A prime example of the government's failure to take the principles of necessity and proportionality to heart is the increasing scope of the National DNA database ("NDNAD"), to include the retention of DNA samples of those persons arrested but either not charged or subsequently acquitted.[30] The genetic information contained in DNA represents the most intimate medical data an individual may possess. The retention and use of an individual's DNA sample without their informed consent, together with the knowledge that an unspecified number of people may have access to that information over an indefinite period via the database, surely constitutes a grave interference with personal privacy. While the legitimate interest in the prevention and detection of crime may justify the retention of DNA profiles of those proven guilty and charged, it cannot be used to justify the indefinite retention of DNA of individuals who are by law presumed to be innocent.[31]

15. Although we predict that it is highly likely that the ultimate effect of these provisions is that UK government will be found in breach of Article 8 ECHR, we reiterate our view that privacy is too important a matter to be left to the courts alone. It is the responsibility of Parliament to ensure that governmental measures affecting privacy are no more than are strictly necessary and that any such measures are carefully tailored to keep any interference with privacy to a minimum.

Inadequate Coverage of Existing Privacy Legislation

16. If Article 8 ECHR by itself is insufficient to provide wholesale protection of privacy under UK law, it is equally a mistake to suppose that existing privacy safeguards, such as the DPA or the Regulation of Investigatory Powers Act 2000 ("RIPA"), are capable of providing comprehensive protection. This is particularly evident in relation to the regulation of CCTV cameras.[32]

17. In 2003, for instance, the European Court of Human Rights found that the lack of any legal remedy for a person whose failed suicide attempt was captured on CCTV and then distributed to the media by the local authority meant that the UK was in breach of Article 8 ECHR.[33] Although the facts of the case show a measure of support for the use of CCTV (the CCTV operator contacted the police), they also highlight the manifest lack of effective regulation for how CCTV is used. Although the DPA governs certain aspects of CCTV usage (specifically the handling of sensitive personal data), it does not provide—and was never intended to provide—a comprehensive legal framework governing CCTV placement and usage.[34] Indeed, it is unclear whether the DPA safeguards even extends to CCTV used for undirected or passive surveillance, since the Court of Appeal has held that "personal data" within the DPA applies only to "information relating to an identified or identifiable individual".[35]

18. Similarly, in our recent report on intercept evidence,[36] we noted that the UK is virtually alone among common law countries in allowing the interception of telephone calls, emails, letters and faxes by authorisation of the Home Secretary rather than by a judge. The framework for lawful interception of communications in Part I of RIPA provides for only ex post facto judicial supervision of only the most limited nature. It is instructive to compare the detailed, open and transparent reports produced by the Canadian[37]

[30] See Sections 63 and 64(1A) of the Police and Criminal Evidence Act 1984, as amended by the section 82 of the Criminal Justice and Police Act 2001 and section 10 of the Criminal Justice Act 2003.

[31] We note that the view we have expressed here is at odds with the 2004 judgment of the House of Lords in *R v Chief Constable of South Yorkshire (ex parte S and Marper)* [2004] UKHL 39 in which the House concluded that the retention of DNA samples of persons arrested but not subsequently convicted did not interfere with the right to respect for personal privacy under Article 8(1) of the European Convention on Human Rights, and—even if it did—was a legitimate restriction under Article 8(2). With respect, however, we consider the decision of the House in Marper to be deeply flawed. We further predict that it is unlikely to be upheld by the European Court of Human Rights on appeal. For further details, see our January 2007 response to the Nuffield Council on Bioethics consultation on the ethical issues arising from the forensic use of bioinformation.

[32] We use the term CCTV generically. As the Royal Academy of Engineering report notes, n2 above, p33: "the term CCTV is now for the most part a misleading label. Modern surveillance systems are no longer 'closed-circuit', and increasing numbers of surveillance systems use networked, digital cameras rather than CCTV".

[33] *Peck v United Kingdom* (2003) 36 EHRR 41.

[34] C.f. the comment of Lord Hoffman in *Wainwright*, n5 above, para 33: "Counsel for the Wainwrights relied upon Peck's case as demonstrating the need for a general tort of invasion of privacy. But in my opinion it shows no more than the need, in English law, for a system of control of the use of film from CCTV cameras which shows greater sensitivity to the feelings of people who happen to have been caught by the lens".

[35] *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

[36] *Intercept Evidence: Lifting the ban* (JUSTICE, October 2006).

[37] See eg Public Safety Canada, *Annual Report on the use of Electronic Surveillance—2005*.

and US[38] federal governments on the use of electronic surveillance with the paucity of information available under the report of the UK Interception of Communications Commissioner.[39] It is equally striking to note the similarities between the UK's system of intercepts without prior judicial authorisation and the system of warrantless surveillance operated by the National Security Agency and recently held unconstitutional by the US federal courts.[40] In our view, the power of the Home Secretary to issue interception warrants for both intelligence and law enforcement purposes should be replaced with a scheme for judicial authorisation of interceptions. This would bring the UK into line with the practice of virtually every other common law country.[41]

21 June 2007

Examination of Witnesses

Witnesses: Mr Gareth Crossman, Director of Policy, Liberty, Dr Eric Metcalfe, Human Rights Policy Director, JUSTICE and Dr Gus Hosein, Privacy International; Visiting Fellow, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, examined.

Q219 ***Chairman:*** May I on behalf of the Committee welcome Dr Metcalfe, Dr Hosein and Mr Crossman. We are not being televised but we are being audio recorded so could I please ask you to state your names for the record and the organisation that you represent.
Dr Metcalfe: My name is Eric Metcalfe. I am the Director of Human Rights Policy at JUSTICE.
Dr Hosein: My name is Gus Hosein. I am a Senior Fellow at Privacy International and a Visiting Senior Fellow at the London School of Economics.
Mr Crossman: My name is Gareth Crossman. I am the Director of Policy at Liberty.

Q220 ***Chairman:*** Thank you. Would you like to make an opening statement or would you prefer to proceed straight into questions?
Dr Hosein: We would all prefer to go straight to the questions.

Q221 ***Chairman:*** Could I ask how you would define, if at all, a "surveillance society" and whether you think we live in one?
Dr Hosein: The surveillance society language has been within academia for a while, which means to say that there is no certain definition. The Information Commissioner's Office started using the language about two years ago, saying that we were sleepwalking into a surveillance society, and at that time we were not too sure if that was a helpful vocabulary. I believe that the common definition would be "pervasive surveillance to which you have no recourse", but we never felt that to be a particularly useful definition or a useful term because it renders the whole debate as though the individual is powerless. We believe that the individual still has rights—under the ECHR, the Human Rights Act, the Data Protection Act—and so we still believe that there is a struggle to be had; we have not given up the fight just yet.
Mr Crossman: I very much agree with Dr Hosein about some of the language that has been used. Traditionally, you used to try and avoid emotive language the subject of an issue that is essentially about proportionality, but now that the language of surveillance society has entered the consciousness, it is useful and appropriate language to use. If I was going to say where I think things have gone wrong, the question of proportionality is very important. Legitimate state interference into individual privacy is, of course, part and parcel of a democratic society, but as a consequence of a number of factors over the last few years, the concept of proportionality, about the need to justify the need for legitimate purpose, the need to only do things in a way which is appropriate to the situation faced, has fallen away from surveillance, whether it be mass surveillance through a database, whether it be through visual surveillance of CCTV or targeted surveillance through the use of the Regulation of Investigatory Powers Act, so underpinning our concerns over surveillance is that the accountability and proportionality elements have fallen away.

Q222 ***Chairman:*** Could I ask what your response is to the news last week in the annual report of the Interception of Communications Commissioner, Sir Paul Kennedy, that over 250,000 requests for communications data were made between April and December 2006, and whether you think that the level of covert surveillance is getting out of control and, if so, how you would address this?
Dr Metcalfe: We are certainly very disturbed by the figures which came out last week. I think there was initially, in the media reports, some confusion between the number of interception warrants, that it is to say, communications actually being listened to

[38] See eg *Report of the Administrative Director of the United States Courts on Applications for Authorizing or Approving the Interception of Wire, Oral or Electronic Communications, 2005.*
[39] See eg *Report of the Interception of Communications Commissioner for 2004* (HC 549; SE/2005/203).
[40] See *American Civil Liberties Union v National Security Agency*, US District Court, 18 August 2006 (Case no. 06-CV-10204).
[41] See our 1998 Report, Recommendation 2, pp 19–22.

for their content, and requests for communication data which is the location and identity of the telephone number that you are calling. Nonetheless, it speaks to the very broad use of surveillance powers that are available under the 2000 legislation. In particular, we are extremely concerned about the lack of sufficient legal regulation for the exercise of those powers. I do not mean by that that there is no legal regulation, the Interception of Communications Commissioner plays a role. But the United Kingdom is virtually alone in every common law country in not requiring prior judicial authorisation of interception warrants and indeed, as we found in relation to buggings in prison, there is no prior judicial authorisation of intrusive surveillance either. There is a limited role in relation to police surveillance in which the Surveillance Commissioners play a role but, for example, if MI5 seeks a surveillance warrant in a prison, there is no requirement to go before a judge and seek an assessment of the proportionality of the request in human rights terms, under UK law as it currently stands. So we are extremely concerned about the lack of sufficient safeguards in this area.

Q223 ***Lord Peston:*** I have a small technical question. Are scale, on the one hand, the size of the thing, and the use of technology, intrinsic to your definition? I will give you an example at the other extreme, which may seem ludicrous, but if you live in a small village, as I do, everybody knows everybody's business. How anybody would ever have an affair is completely beyond me; we all know what everybody is doing all of the time. The idea that this is somehow the Stasi writ small—as that ludicrous article by Mr Heathcoat Amory asked us to believe generally about our society—we would regard as preposterous. In other words, knowing everybody's business is not somehow incompatible with privacy on a small scale. But what you are saying is, if I am right, that on a large scale and using technology then it becomes a problem?
Dr Metcalfe: I think it can be.

Q224 ***Lord Peston:*** For example, in the House of Lords, we all gossip about each other all the time, but I do not think we think we are living under a Stasi-ist regime here, even though most people know everything about everybody.
Dr Metcalfe: I would not adopt the description of the Stasi-like situation. I would not agree with that. I do agree that scale definitely matters, for example, with medical reports. Traditionally, your medical reports are held by your local GP and we have many examples of cases where there is very poor security around those medical records. However, once you put those medical records onto a national database, which is accessible from a wide number of points throughout the United Kingdom, then you encounter problems of scale and technology.

Q225 ***Viscount Bledisloe:*** As I understand it, there is a distinction between interception of communications by telephone and overt listening to direct conversations—I would call the latter "bugging". Is there any control over that? If you come to my house and I put a bug to record what you are saying, or if I go to prison and the prison puts in a thing to record what I am saying, is there any control over that or at the moment is one free to do what one wants?
Dr Metcalfe: There is legal regulation, it is the Regulation of Investigatory Powers Act 2000, which is the primary legal framework governing both surveillance by law enforcement bodies and interception of communications. It is true to say that there is a distinction between listening to a private conversation, or intercepting a private conversation, because you are concerned with the contents, say, for example, the contents of a letter, the contents of an email, what is actually said in the telephone conversation, and surveillance by way of a listening device which is external to the communications, say, for example, a listening device in someone's home or office or even their vehicle. The distinction tends to blur somewhat, and this is a loophole that we have identified in the interception regime, because it is perfectly possible to have an external listening device that records someone using a hands-free device with their mobile telephone, for example, and we quite often find this in criminal cases where interception evidence is inadmissible due to Part 1 of the 2000 Act but, nonetheless, if you happen to record someone speaking into a telephone by an external device and with a hands-free device if you record what is coming out of the speaker, that is admissible.

Q226 ***Viscount Bledisloe:*** I am talking about actual direct conversations without the use of any machine at all, putting a bug under the dining room table so that you can record what people are saying at dinner or, as has been suggested, putting a bug in a CCTV camera in a shop so that you can hear the conversation. Is there any control on that—done by a private individual?
Dr Metcalfe: A private individual who intercepts a private communication commits a criminal offence.

Q227 ***Baroness O'Cathain:*** Even in his own room?
Dr Metcalfe: You can intercept your own conversation, but if you intercept someone else's conversation, a private conversation between two other individuals, you commit an offence.

Q228 ***Viscount Bledisloe:*** If I, without telling you, record what you say to me, that is all right?

Mr Crossman: It is important to make a distinction here between interception of communications and listening. Interception of communications, if you intercept someone else's communications you commit a criminal offence. If you are listening in on other conversations, you are not necessarily, depending on the circumstances in which you might do it; there might be some civil action involved.

Q229 ***Viscount Bledisloe:*** What is the difference between intercepting and listening in?
Mr Crossman: It is not just the difference, it is who does it as well because it is the distinction between a state agent doing it, in which case it falls under the Regulation of Investigatory Powers Act, and private individuals doing it, which might fall under the Data Protection Act, or might be unregulated depending on the circumstances. The reason there are so many problems in this area is because we have this statutory framework, through the Regulation of Investigatory Powers Act, which is a framework but it is phenomenally complex. There are five different types of surveillance from interception through some of the mid-range types of surveillance, such as intrusive surveillance, directed surveillance, human covert surveillance, down to communications data. As well as having these different levels, you have different people having access, different authorisation mechanisms, different post-events accountability mechanisms. My belief is that the reason we have this Byzantine system is that when the legislation was passed, rather than taking a view as to how we should put together a comprehensible and accountable mechanism whereby people who are exercising these powers know which system to follow, with proper judicial involvement for the highest level of authorisation, what in fact happened was that the legislation was built around the existing framework which had been built up over a number of years in a piecemeal way, making RIPA one of the most phenomenally complex and difficult pieces of legislation to follow. We believe very strongly that there needs to be a wholesale review of RIPA, I think the events of last week may now make that a stronger case, and that there needs to be a much greater accountability mechanism.

Q230 ***Lord Rodgers of Quarry Bank:*** Going back, if I may, to these comparisons with the Stasi state, in the particular article which many of us have read by Timothy Garton-Ash, describes some of what he calls "the necessities of having dykes of the tide of surveillance", refers to the need to tear down in the name of terrorism, crime, fraud, child molestation, drugs, religious extremism, racial abuse, taxation, etc., fly-tipping and too many garbage bags, and the apparent logic, as I would see it, that the surveillance state is becoming a "nanny" state. Would you share that view, or would you think that what Timothy Garton Ash says is a good deal of hyperbole?
Mr Crossman: There is a great deal of hyperbole. I do not think hyperbole helps, which is why I always try to avoid phrases like Orwellian, 1984, Big Brother, because I do not think they help with legitimate criticisms. If you take an issue such as the profiling of information, which is where you basically process data without human intervention to see whether it fits in set parameters. That could be done for the most absolutely legitimate reason such as, for example, taking census information to determine a particular area where there might be social exclusion requiring the targeting of resources. I do not think anyone would argue with that as being a perfectly legitimate use of profiled data. Similarly, you could use profiled data for criminal justice purposes. The Home Office have said that they see this as being a legitimate way of determining whether or not crime may be taking place: no human involvement, just the profiling of otherwise innocuous data to see if some anomaly might throw up some criminal activity. Now, you are doing the same thing, but it is the purposes for which you do it, so if you are talking about nanny stateism, it depends whether you think that is a good thing or a bad thing. Is nanny stateism ensuring that people do not fall through the net or is it basically placing too much emphasis on unjustified state control? It can be both. The legal mechanisms are in place, it is the policy drivers of the Government that determine how they are put into effect.

Q231 ***Lord Lyell of Markyate:*** Just to try and pin down the ambit of what we are dealing with, the five different methods of surveillance that you outlined are set out in paragraph 53 of the first paper we received from the Ministry of Justice and, as you say, they deal with phone tapping, telephone call records, bugging in private accommodation, catching people out in the open with these special microphones, and covert entry onto private property and interference with private property. Does the 250,000 figure given by Sir Paul Kennedy cover the whole lot of this, and how does it break down between them? Can you give the Committee some idea of the extent of each of those that is going on?
Mr Crossman: The vast majority, in fact, the one you did not mention, which is communications access; data access, which is the lowest level of surveillance; email traffic; mobile traffic; telephone traffic, not the content but just the record that they were made, that accounts for the vast majority and it is authorised at a very low level, for example, by officers within local authorities. I think the question that was asked earlier was, were we shocked by the number that there were? No, because even though it might have been a news story, the Interception of Communications Commissioner's reports for the last

few years have shown the levels have remained relatively constant, at about 300,000 to 400,000 applications a year. The much smaller quantity is the higher level—the intercepts and the bugging—they run into thousands a year, rather than hundreds of thousands. It would be very misleading to be giving the idea that there were hundreds of thousands of buggings, or interceptions, taking place every year; those account for a very small number of the total.

Dr Hosein: We were talking about 200,000-plus accesses to communications data, although it is treated by the law as relatively innocuous information, this information is quite detailed. It is every location where you use your mobile phone, or where you are taking your mobile phone. It is every interaction you have done online, which is stored by the internet service provider, it is every phone call you have ever made in the past two years and where you were when you made that phone call. It is very detailed information. The advocate in me says that this is highly sensitive information that can show a map of your private life. But the academic in me would note that the vast majority of those accesses—the 250,000 accesses by local authorities and government departments—are usually just for subscriber information. That is, who was in this vicinity at that moment? So they go through all the mobile phone records to identify the individual. They do not ask who was calling, they just want to know who the individual was. Who just called this Government authority? Well, we will go to BT and find out who owns that telephone number. It is that kind of data. That is not to say that matters are going to get worse, but I am saying that is what it is now because the local authorities and the police are not fully aware of their own powers to get access to the type of data that is being retained under terrorism law in this country.

Dr Metcalfe: Just to clarify about the numbers, Mr Crossman referred to interceptions, which are the most detailed, the most intrusive type of surveillance in relation to private communications. The numbers have remained relatively stable, somewhere between 1,700 and 2,000 interception warrants are issued a year. However, it is worth noting that the numbers can be slightly misleading. An interception warrant can target one of two things. It can target either a named individual, so all of that individual's private communications can be the subject of a warrant, that is to say, all my telephone calls, all my emails and all my text messages, and so forth. Or, it can refer to a single premises, which means that if you seek an interception warrant for, say, for example, the newsroom of a national newspaper, you would capture all the people working in that office and all their private communications to and from that premises. So, in fact, the number of private communications being intercepted may not be accurately reflected merely by the number of warrants. However, I would agree with what has been said, the much broader number refers primarily to communication data and a far smaller number refers to the number of actual interception warrants given out.

Q232 ***Lord Rowlands:*** I think it was Dr Metcalfe who said that we stand out as a small minority which do not apply prior judicial warrants. I do not know the history of our legislation. What case has been made out for being different?

Dr Metcalfe: We did a very detailed report in 2006 on interception of communications which is probably the paradigm case, where the security service and the intelligence services have always been extremely keen to keep judicial and legal proceedings to a bare minimum because they are extremely concerned that allowing intercept material to be used in court, for example, would disclose methods of interception. Why they would resist prior judicial authorisation, I think, similarly, there is a concern to keep the number of people who need to know the information to the absolute minimum. There has been a very strong history of political authorisation going back to before 1640: one of the earliest Home Secretaries made interception in the 17th century to authorise the interception of mail. It is a very longstanding practice of political authorisation for interception of communications. There is limited independent authorisation for police surveillance, but otherwise I would say that the history of this country has been much more comfortable with political authorisation. The interesting comparison is with where we require judicial authorisation. A search warrant of your house would require a magistrate, so for someone to come into your house and search your premises, it would require a magistrate. However, if MI5 wants to place a bug in your house, for example, that can be done as a warrant by the Home Secretary. We do not think that is a very good situation to be in.

Q233 ***Chairman:*** Before I call on Lord Norton, could I ask what your view is of the so-called Wilson doctrine, which is opposed by Sir Paul Kennedy and many others, that Members of Parliament and Peers should not have their communications interfered with by anybody.

Mr Crossman: It is a good general principle, in that there are certain people such as parliamentarians, such as lawyers, who would expect as a matter of principle that they are not subject to surveillance, whether or not it be a doctrine, as in the Wilson doctrine with no legal base, or on a more formal legal basis such as communications between lawyers and clients. That is not to say I think it should be an absolute. I believe that with any individual—whether they be MP, lawyer or member of the general

public—if there is a suspicion that they are involved in criminal activity and there is justification for surveillance, that there should be a bar on that. What has happened in the last week has been extremely useful, especially for the likes of organisations such as ourselves who try and raise interest in these issues, that the events of last week have shown the problems that there are with the current process. I would not, however, want it to become "about the Wilson doctrine". From our perspective, it is not about parliamentarians in particular, it is about the 60 million people in this country who are not parliamentarians and they are not protected by any particular doctrine.

Dr Metcalfe: I agree with what Mr Crossman has said. We agree with the general principle and the Wilson doctrine reflects a sensible, rather sound public interest in ensuring that Members of Parliament and Members of the House of Lords are able to carry out their business without fear that they are likely to be surveilled. This is particularly true because what you are more likely to be discussing in your private communications or communications with the general public is likely to be of more interest in intelligence terms, even in very general terms, than the conversations of ordinary private individuals. That said, I do not think it is necessary to frame it as a blanket prohibition, if there is real and compelling evidence that a Member of Parliament, for example, was involved in serious criminality, I do not see why it would not be possible to seek authorisation for an interception of their communications, so you would fall back on the general point that a sound case has to be made out. This is an example of the doctrine which reflects privacy as a public good, which is a point we had made in our written evidence. This is the idea that privacy not only serves the interests of the individuals themselves but it serves the interests of society as a whole. There are other examples of this: Members of Parliament are immune from suit in relation to statements they make on the Floor of the House. That reflects similarly a public interest in making sure that Members of Parliament are free to speak their minds without fear of suit. It reflects the idea that there are good public policy reasons for protecting individual privacy, not merely the individual self interest.

Q234 ***Lord Norton of Louth:*** This really follows on from that and to some extent Dr Metcalfe may have previously answered the question because in your evidence, if we look at the fundamentals of why this matters in terms of public interest versus individual right to privacy often they are seen as mutually exclusive but your argument you just developed is that in fact they are not, the individual right to privacy is also a public good. Do you want to develop that and also explain whether you think there are cases when one can make a public interest argument for violating the right to privacy and if so, the fundamental question is, where do you draw the line, what is the basis on which one does that?

Dr Metcalfe: Let me answer the last part first. I certainly agree that there are cases where it is in the public interest to interfere with an individual's privacy. Unfortunately, the argument that I am making does not actually add any additional means for identifying or resolving the difficult conflicts that will arise. What it does and the reason why we presented the argument was because we are very concerned that the argument is very much framed in an oppositional state public interest versus the individual private interest. The point that we were trying to make is that the individual not only benefits but society as a whole. In fact, in a more basic and rather more abstract and philosophical sense, privacy matters to the exercise of our freedoms, of our ability to be autonomous. We tend to make our most important decisions not on the public stage but in private, which is why we deliberate privately. Voting, is a very good example—a primary democratic right—it is something that we do in secret; we are free to disclose how we voted. The opposite case is Members of the House of Lords and Members of Parliament who vote in public. The principle there is that you are representing a public interest, or in the case of Members of Parliament, an individual constituent, so if I vote for a Member of Parliament, I am entitled to know how they voted in the House. But my own vote remains private. The idea is that society as a whole benefits from individuals, each individual having his own privacy in their personal affairs. By contrast, if we remove that, or if we interfere in that too much, then we lose the benefits which flow from that as a whole.

Q235 ***Lord Norton of Louth:*** To pick up on that point, which you say anyway is almost a philosophical point rather than a practical one, is it not the case that the argument for public good reinforces the importance of the right to privacy and therefore is a case for the height of the threshold that you impose before that right can actually be violated? In other words, it is in the interests of society not to violate the individual's right to privacy and therefore it is a case that just reinforces the high threshold.

Dr Metcalfe: Absolutely, and in particular, for us it reinforces the need to have very tight, very clear restrictions on when privacy can be interfered with. If, for example, you do not have prior independent authorisation in cases of directed surveillance, then it is a problem.

Q236 ***Lord Peston:*** Could I read out, because the wording is important, some written evidence from JUSTICE: "the government frequently seems more

concerned with whether it *could* establish a new database, etc., and not with the more important question of whether it *should*". I would like some clarification of that, starting with the *should*. Wearing my academic hat, *should* could mean at least two things, one is whether it is ethically right or whether it serves a valuable purpose. Which did you have in mind when you were using that *should*?
Dr Metcalfe: I think I was aiming at the normative aspect of it. I am concerned with the ethical considerations.

Q237 ***Lord Peston:*** So, you are not saying that they should first ask whether this database serves a valuable purpose.
Dr Metcalfe: If you look at the legal test, the proportionality test, establishing legitimate purpose is part of that exercise, so I would tend to roll that together in the proportionality question.

Q238 ***Lord Peston:*** Going back to the *could*, I read *could* to mean whether it was technically possible to set up this particular database, but one of my colleagues interpreted it to mean whether it was legally the thing to do. Which did you have in mind?
Dr Metcalfe: When we wrote our evidence I had in mind your meaning, however, I can certainly consider the additional question. Obviously the Government would not want to introduce something which it considered unlawful.

Q239 ***Lord Peston:*** Does this then amount to a general view that whether it is a new database in the broad sense, and I am quite interested in what is a database as you could tell from my earlier question because I would [not] regard the six pages in my diary with names, addresses and telephone numbers as a database: if I put them on the computer it does not suddenly become a database where it was not one before. So you are really talking not about databases in any small sense, you are really—to go back to my earlier question—talking about something big always when you are discussing this?
Dr Metcalfe: It is the collection of information.

Q240 ***Lord Peston:*** On a large scale, though.
Dr Metcalfe: On a large scale.

Q241 ***Lord Peston:*** Let me give you an example, if we were to go into the private office of any government minister, except that it is usually a mess, but in theory they have got a great number of phone numbers, telephone numbers, and a whole lot of records, but that is not what you have got in mind when you are worrying about this kind of problem is it? I am trying to get to the basis of what it is you want us to focus on.
Dr Metcalfe: It is a question of core principle as well as a question of scale. Private individuals can collect information. I can stand on a street corner in the village that you refer to and make a note of the comings and goings and that, in and of itself, my private legitimate act, or at least lawful act, can in doing so gather a lot of valuable information which people might not want to be disclosed. However, we are talking matters of scale when private companies collect information and also when governments collect information. Governments obviously have the power to request and indeed require a great deal more sensitive information about private individuals than I can standing on a street corner.

Q242 ***Lord Peston:*** Yes, of course, but that goes back to the scale point and you have made that point. I am really just trying to understand from this particular question what it is you want us to focus on because, after all, the outcome of all this will be a report at some stage. Is your view that when we are looking at databases, and we will accept that we are now talking large-scale, and first and foremost government, what we ought to focus on is individual rights in this matter, that should always be a focus when we are looking at it, and within those rights the particular right to privacy. If I were asking what your philosophy of all this is, would that be a fair summary?
Dr Metcalfe: That would be a fair summary.

Q243 ***Lord Peston:*** But it would not then rule out the creation of databases, it would question every database in those terms.
Dr Metcalfe: Absolutely.
Lord Peston: That is very helpful.

Q244 ***Lord Morris of Aberavon:*** In JUSTICE's written evidence, you said that "the common law right of privacy has remained significantly underdeveloped" in the light of new technologies. Why is that and how would you define the common law right to privacy? It seems to me that one of the strengths of the common law has been its adaptability. The same law that applies to horse-drawn carriages as to motor cars, and one could give dozens of illustrations. Why has this come about? Why has the common law not kept up with this need?
Dr Metcalfe: As we indicated in our written evidence, it was not that the common law had not been concerned with privacy but it has not been felt necessary to address or protect privacy by means of overt rules, it has primarily been a matter of non-regulation. It has been interesting, since the Human Rights Act, in particular, to see the development of common law in this area. You can trace a very interesting line from the Earl Spencer case in 1998, when the European Commission on Human Rights,

as it was then, indicated that it thought the law in relation to breach of confidence in the United Kingdom would be sufficient to protect individual privacy rights. Then you had the *Douglas v. Hello!* case in 2000, and more recently the cases of *Douglas v. Hello!* 2005 in the Court of Appeal and *Campbell v. Mirror Group*. We find the courts are now beginning to develop the traditional common law breach of confidence principles and use that to act as a more general remedy for breaches of a person's Convention rights since the Human Rights Act came into force. I would certainly say that the common law is now being used in a way to develop and protect individual privacy. What is interesting is that it took the incorporation of the European Convention on Human Rights into our domestic law to actually prompt that development. Traditionally, I think judges have been reluctant to use the common law to fashion a broad-based common law right to privacy, primarily, on democratic concerns because they feel that, if I understand it correctly, it is more a matter for Parliament. Privacy involves the balancing of so many interests across so many different areas—banking; collection of personal information defamation; the balance between the right to free expression and personal privacy—that they felt that the common law was not a very good tool. Still a criticism can be made that the law in relation to breach of confidence, while it is increasingly used as a remedy in relation to privacy rights here in the United Kingdom, it is perhaps not sufficient. In the most recent House of Lords case, Lord Nicholls describes the breach of confidence as being better understood as a tort of the misuse of personal information. That is a welcome development. The concern, however, is that even framing it as a misuse of personal information, it does not quite go far enough because the ingredients of the tort are still relatively closely defined and not as broadly defined as we might like. When I spoke of the common law by the way I was not merely referring to the role of judges, I was referring to our common law tradition, which is also the way in which Parliament writes its laws.

Mr Crossman: Privacy is such a huge area that it is often very disparate areas. There is very little relationship between the development of the common law of privacy in relation to the application of Article 8 to media privacy and breach of confidence, which is an area heavy in case-law, there has been a lot of case-law about it, compared with what other aspects of privacy you might be talking about such as mass informational surveillance. Common law through the courts has been well developed in the former area, because it is about an individual's rights. When you are talking about mass informational surveillance, it is very much more difficult to pin the tail on whose rights are being involved because if you take the application of Article 8—the right to privacy—it impacts on a very large number of people, but only in small ways, such as information being passed around about them maybe in an excessive manner. The way the Human Rights framework works is that you need to be a victim in order to bring an action, so that if you are talking about someone subject to a control order, for example, it is very easy to identify who the victim might be in order to bring a Human Rights Act case. That is why there has been little common law development with the exception of a few cases, it has not been an area which has been particularly developed. My view is that for specific areas you need to have more Parliament-led statutory basis for regulation through improved data protection laws; through formal statutory regulation of CCTV; through review of the way that regulatory investigative powers work. That is a far better focus for statutes than it is through common law development.

Q245 ***Chairman:*** Before I call Lord Lyell, could I ask whether you think that it would be in the public interest in this country for the Government to be required to undertake privacy impact assessments, as in the United States and in Canada?

Dr Hosein: I think that would be a highly recommended step forward. Australia led the way in rights impact assessments, followed by Canada and the United States. However, there is still the ability to write a privacy impact assessment on a highly invasive system and make it all make sense. For instance, the US visit system in the United States, that fingerprints all foreigners visiting the United States, stores those fingerprints for 100 years and stores the biographical data for 75 years, has a privacy impact assessment. It checks all the boxes and complies with the rules of the US Government but we would also argue that it does not protect privacy in any way. We have seen a regulatory impact assessment for the Identity Cards Act that also disclosed very little. So, in order to make privacy impact assessments work, we need to make sure that the requirements fulfil the purpose of the impact assessment, which is properly to assess the privacy issues and the data protection issues even when they might differ.

Q246 ***Lord Rowlands:*** Some of the members of the Committee are going to Canada and the United States; are there any other illustrations of practices in either of those countries on which we should particularly focus?

Dr Hosein: What is most interesting about the comparison with other countries such as the United States is the high-level public debate. Let us use, for example, the current controversy as to whether or not the President can authorise interception of

communications of suspected terrorists whether in the United States or abroad. That is causing a constitutional crisis. Yet, as we have discussed so far this morning, that is the law of the land in this country. It is interesting to see the differences in political culture in how that reflects the law. In comparison, much is said about how awfully the United States has conducted itself on surveillance issues since 11 September 2001, but for what it is worth, on the surveillance issue, it has generally been more regulated than the conduct of UK and EU Governments.

Lord Rowlands: But equally, if any of you had any information that would help us to prepare for our visit, we would be grateful.

Q247 ***Viscount Bledisloe:*** But if it is totally unclear in this country what is or is not the right to privacy, it would be very difficult to make a privacy impact statement, would it not?

Dr Metcalfe: It is clearer now with Article 8. As Mr Crossman indicated, common law rights for breach of privacy are centred around private individuals and confidential information which they have identified as confidential, and most of the case-law has related to celebrities and newspaper or media groups, so we are talking about the development of a very small area of the media pool. Mr Crossman indicated very broadly that there are many more issues in relation to that. Article 8 cuts across the board and provides a very good general principle establishing the right to privacy. The difficulty with Article 8 is that for members of the Council of Europe, it does not specify the particular legal principles that you have to adopt because it is written to embrace both civil law and common law jurisdictions. To a certain extent, civil law jurisdictions, based on Roman law and Napoleonic law, are slightly more comfortable with the regulation of personal identity because their legal systems are structured differently, whereas in this country, as we referred to in our written evidence, you have a tradition of simply protecting privacy by not regulating it; by not legislating in ways that interfere with it, and that provides the real challenge.

Q248 ***Lord Lyell of Markyate:*** How can Parliament act as a restraint on "the executive's enthusiasm for the administrative benefits of surveillance and data-collection", which you urge in your very good paper; how can it do it in practice? I have one suggestion to make in a moment.

Dr Metcalfe: I am not sure that it can restrain the enthusiasm any other way except by refusing to pass laws in relation to those areas, or refusing to pass disproportionate laws. The obvious check that Parliament has over the executive is in the making of laws. The executive can propose them, but it is for Parliament to decide ultimately what laws are made, and to scrutinise those laws very closely in terms of their proportionality and, going back to the basic point, the necessity. Is it actually necessary, for example, to create a national identity card?

Q249 ***Lord Lyell of Markyate:*** Can I suggest to you that the way to do it—there is this awful word "transparency" but it is to make it obvious who is responsible—before one is surveilled or one's property is entered, or whatever, that some minister or public official has to be responsible for giving the authority, and they can be seen to have done that and they can be criticised if they are disproportionate. Would that not be a good protection?

Dr Metcalfe: It would depend on the kind of interference that we were referring to. Obviously, in some cases—and interception is an obvious one—there will be very good reasons: you would not want to make an interception warrant public, or you could not make the terms of it public without losing the obvious covert benefits that come with that. With other kinds of authorisations, for example, it would be a lot better if there was a specific database of decisions in relation to the placement of CCTV cameras. So, I agree that greater transparency as a whole is a very good general principle. The difficulty I have in answering that question is that a lot would depend on the particular kind of interference in the particular area we were talking about.

Dr Hosein: One way we could enable Parliament to view these issues in a clearer way is to see it as a public policy issue and perhaps, controversially, not as a rights issue and not as a security issue. The ID card is a great example where ID cards were promised by the Government as a security issue and so therefore opposition to ID cards was, "oh, you're interested in a selfish right of privacy in favour of the state's need for security". Instead, if you approach it as a public policy issue and ask, "Can you build this database? How much will it cost to implement this system? What are the ramifications across Government and the private sector?" Then you will see that often, as we have found over the past 15 years, when you design privacy into the development of law and technology, the technology becomes more feasible and more likely to work. When you do not design it in, that is when they start falling apart and you end up with these massive databases that can never be built. To recap: see it as a public policy issue first, with the connotations of security and individual rights.

Mr Crossman: There is one very specific constitutional suggestion that I would make in response specifically to that question. Whenever legislation is passed, Parliament has been able when considering privacy to determine of proportionality: what is the appropriate exercise of these powers by different bodies. What you find when you look at

pieces of legislation with privacy impact is that frequently you will see that what has happened is that Parliament is asked to pass the framework for primary legislation; the detail as to who actually exercises these powers and what powers are exercised is reserved for secondary legislation. As, of course, you will all know, secondary legislation goes through on the Aye or the Noe. You do not, as a Parliament, have the opportunity to consider if you have ten public bodies who are to be given these powers, eight of them you might say, "absolutely appropriate, but I am not happy with these two. I think that would be disproportionate." There is no constitutional reason whatsoever why Parliament could not be permitted to determine to amend resolutions. There are two precedents for this: first, in the Civil Contingencies Act, Parliament has the opportunity to amend resolutions passed under this Act. Early drafts of the Identity Card Act had the ability for Parliament to amend resolutions in relation to determinations by the Secretary of State as to who was designated. So, there is no constitutional basis why this cannot happen. I would suggest that it is absolutely appropriate when Parliament is being asked to consider which bodies have exercise of which powers, that they be able to make a determination as to which of those it is appropriate to have. The reality is that does not happen because Parliament is simply given a piece of secondary legislation and asked to approve or disapprove it.

Q250 ***Baroness O'Cathain:*** Mr Crossman, to you again, your written evidence says there is no justification for the National Identity Register associated with the Identity Card Act. But on the other hand, you said that there is justification for other information on a database such as the Children's Index, which is now called, Contact Point. Can you explain why you draw this distinction?
Mr Crossman: Absolutely. I should start by qualifying the first part of the comment. At Liberty we look at things essentially from a human rights perspective and when you are dealing with a qualified right such as Article 8—the right to privacy—you look at it in a qualified manner that you will not do if you are talking about an absolute right, such as the prohibition on torture. For a starting point, I would not say, "there is no situation whatsoever in which a national compulsory identity card scheme could be justified". I cannot say that as an absolute. To do that would be to necessitate saying that the previous scheme—the wartime scheme of compulsory national identification—was not justified. I do not have an opinion as to whether it was, I suspect it might have been, so I do not take an absolutist position on this. What I would say is that this scheme, proposed as it was with the justifications that were given for it and the societal consequence that I believe would flow from it, was unjustified. There is a distinction there between saying that you cannot justify a particular type of database and saying, "is what the Government is proposing justified?". In relation to the Children's Index, I would say that there is perfectly legitimate basis for a limited database of children who have been identified "at risk" to be stored with appropriate access for those individuals who might have responsibility for their care. What the Government proposed originally—it has been limited somewhat as it has been whittled down—was a mass informational database of every single child with very random entry criteria, such as causes for concern—whatever that meant—with a huge amount of public access to it which my belief was not only had privacy implications but would prove to be counter-productive, in that anyone working with children, because this came out of the death of Victoria Climbié, anyone working on the coalface of Social Services is always going to record information for fear of being the person who did not record something, information overkill, meaning that you cannot see the wood for the trees, and those children who are genuinely at risk being overlooked because there is so much data. That is why, for me, proportionality, legitimate purpose, is at the heart of approaching any particular database.

Q251 ***Lord Rowlands:*** But is this not going to be, whether you like it or not, subjective? Dr Metcalfe, earlier on, mentioned I think in a critical fashion, the collection of medical records on a central basis. I would find personally particular comfort from the fact that my records are on a central basis so that if at the weekend I had an accident, somebody could access immediately what medication I was on when I might not be able to tell them and therefore they might not make mistakes. I would not object to that. So how does the individual subjective view of whether we want to be on databases link in to this whole idea of proportionality or indeed whether we should or should not have them?
Dr Hosein: You would begin by letting individuals choose to be in a database or not to be in a database. It is a whole opt-in process.

Q252 ***Lord Rowlands:*** Opt-in, not opt-out?
Dr Hosein: Yes, opt-in. I do travel a lot on weekends and I want my file on the database. But that does not mean the database ought to be designed the way it has been designed, which is potentially 400,000 people across the country would have access to your medical records. There are ways of designing this technology so it limits what is absolutely necessary to hold the net record and limits who has access to it under what circumstances. But that is not how it is being designed now.

Q253 ***Lord Rowlands:*** But if I had criminal intent I would certainly not opt in. How do you run a voluntary database when many of those who would not want to be on that database for illegitimate reasons would not obviously volunteer or contact?
Dr Metcalfe: I think it goes back to the points about necessity and proportionality and there is obviously a difference in, say, a criminal database where people have been convicted of criminal offences. Their choice as to whether their records should be stored is obviously going to be non-existent and this is down to public policy reasons. Whether medical information should be stored is for a completely different reason. I should just make clear my point about the objections to the medical records database is not to the principle—I agree with you there are very sound reasons why you would want to have your medical records available electronically and if the option comes it is one that I would think strongly about exercising. But it should be my choice.

Q254 ***Lord Rowlands:*** So the principle of opt-in is the thing?
Dr Metcalfe: The principle of opt-in but that would be case-by-case. That would not say that is necessarily the model you would follow for every database. There are some databases for example, the National Identity Register, even though I accept that there are legitimate purposes in its creation and there are doubtless useful benefits that will flow from its creation, it is simply not necessary. It is not necessary to store that massive amount of personal information.

Q255 ***Baroness O'Cathain:*** On opt-in and opt-out, what nobody has yet said is that people will not have the necessary information to know whether they should opt in or could opt in. Everybody in this room would almost certainly know what was going on and say, yes. On this latest example of organ donor, I am sure all of us would know what to do about opt-in and opt-out, but ask any ordinary Joe Bloggs in the street about opt-in and opt-out of a donor organ system, how would you get the message across? In order to cover the points that Lord Rowlands made about the medical database and he being on holiday and his medication being known, is it not better to do it on the basis that everybody should be on it.
Dr Metcalfe: Again, this comes down to the case-by-case point and I think there are very good reasons for having an organ donor system which is opt-out and a medical records system which is opt-in. One obvious distinction which can be drawn is that once you are dead you do not actually have particularly strong interests or the interests that you would have tend to be outweighed by the interests of the living. In relation to medical records, we have had very detailed conversations with the NHS on this. Our disappointment is that there is an obvious opportunity for a public information campaign.

Q256 ***Lord Peston:*** I disagree very strongly with your remarks on opting-in and opting-out of medical records. If you go to the excellent walk-in NHS clinic just opposite the Army & Navy, which is a superb walk-in place where you can get some treatment for all sorts of things. You go in and you are asked to provide information about your medical condition. When I went the first time I said, "But look surely you just log into my GP and you will get my medical records?". They said, "No, we are not allowed to do that". So, I said, "what do you do?" "Well, I am now going to ask you about your whole medical history." So I sit there for 20 minutes giving them my medical history, so we waste that 20 minutes, which is what you think is right. But supposing I say to the doctor who was seeing me, "oh, I am exercising the right of privacy here, I am not going to tell you my medical history", which is what you are saying I would have the right to do. How is the doctor to treat me remotely? The doctor would just think I was barking mad. I would have thought in any rational society the one thing that ought to be available to all legitimate people, namely the medics, is a patient's records; they ought to be there, and I find your position extraordinary, that you would advise people of their rights to opt out of telling a doctor what their medical condition was. It is barmy, and I think that most people would regard it as barmy.
Dr Metcalfe: It would be barmy if you were in a situation of seeking treatment to refuse to tell the GP.

Q257 ***Lord Peston:*** But why am I going to see a doctor?
Dr Metcalfe: Your reason for seeing a doctor may be completely different. Let me put it to you this way, in order for the doctor to give you any kind of treatment, the doctor has to obtain your consent and not merely your consent but your informed consent. Why should you need more informed consent for sticking a needle into someone or performing a minor surgical operation, than the informed consent that should be involved in transferring your individual personal sensitive medical information to a national database? If you can obtain informed consent, and doctors are well skilled at explaining complex medical procedures to patients, it is hard to see why they cannot take five minutes to explain the consequences of transferring medical records.

Q258 ***Lord Peston:*** Have you had any recent medical experience, personally?

Dr Metcalfe: With going to a doctor? Well, yes.

Q259 ***Lord Peston:*** I will give you an example, when you are in hospital you are always asked for your date of birth because that is used to identify all the treatments you are getting. Now, supposing I exercise the right to privacy and say, "I'm not going to tell you my date of birth", and then they cannot identify the drugs that they have to give me. I really think that taking this right of privacy in this area is taking us well beyond what any rational person would think was sensible. I wanted you to emphasise your philosophy in my earlier question.
Dr Metcalfe: It is an extreme example of someone refusing to share information with their consultant physician, but the point I would make is that individual bears the cost, if they irrationally refuse to provide their treating physician with the information they need, then they themselves bear the cost.

Q260 ***Lord Peston:*** The alternative view, and I used to be an expert on public good, is that your approach to this matter brings the right to privacy into disrepute.
Dr Metcalfe: No more so than the right to refuse medical treatment.

Q261 ***Lord Peston:*** I should not really be arguing with you.
Dr Hosein: I just think we are approaching this from a slightly wrong perspective. What we are talking about is, of course, as an individual patient moves around the system, it would be ideal if his or her medical records followed accordingly. Instead, what is being designed is a centralised database of all the medical records of all the people in this country, without their consent, made accessible across the NHS and other Government departments to 400,000 different types of civil servants who can get access to your medical records. That is a design issue, and that is wrong. If we could design something that made it completely possible for an individual to carry around say, a medical card that carries the record from office to office to office and discloses only what is necessary to that doctor or that hospital, that is fantastic, but that is not what has ever been considered.

Q262 ***Baroness O'Cathain:*** We have recently had some very good evidence from people dealing with the DNA database, so what additional legal and ethical safeguards would you suggest for the national DNA database?
Dr Hosein: I believe all of our organisations have been involved in the *Marpa* case as it goes to the European Court. We submitted a brief to the European Court discussing some solutions to the current problem. To answer your question directly, I believe that a complete rethink is required. If I was forced to come up with a solution for the DNA issue for the police, it would be to create a database of all the cold cases—with all the evidence left at scenes of crime over the years—and create a DNA database of that. As you arrest and charge people, you can take DNA to verify against that database, but there is no need to collect the information arbitrarily based on just being arrested and retaining it indefinitely—I do not agree with that. Dr Helen Wallace, who, I believe, has spoken; she is our adviser on that issue.

Q263 ***Baroness O'Cathain:*** Could we have a copy of your submission to the European Court, because I do not think we have had that?
Dr Hosein: I am not sure that we are allowed to.

Q264 ***Baroness O'Cathain:*** It just might help us to concentrate our minds.
Dr Hosein: I would love to and if I can look into that, I will definitely come back to you.
Mr Crossman: You asked a question about the legal regime and there are some specific changes that I would make to the current regime as we have it in order to, in my view, make the current retention of DNA more proportionate. In recent years there has been roll-out of the national DNA database so that permanent retention of DNA samples is allowed from anybody who is arrested for what is called a "recordable offence". A recordable offence is an offence which carries a sentence of imprisonment, even if you do not get sent to prison. So, from a very minor offence or some other non-imprisonable offences such as begging, if you are *arrested* for any of those offences and actually charged, you can have your DNA permanently retained until you are 100 years old. There is really no statutory basis for getting rid of it; that is where the problem lies. It is very open-ended, it is left to the discretion of individual forces, who apply it on a rather arbitrary and piecemeal basis. The default position is not to delete samples of DNA, they only tend to be deleted when an individual is so bloody-minded about it that they continue to push and push until in the end the individual police force gets rid of it. That is not a satisfactory basis.

Q265 ***Chairman:*** I have received an extremely helpful suggestion that if possible Liberty's view of the DNA database might be sent to us on paper, in the interests of time marching on.
Mr Crossman: Absolutely. I have passed a few copies of the report around which probably contains all the information you need.
Chairman: Could I make a traditional Chairman's appeal for brevity in answering questions.

Q266 ***Lord Peston:*** Again, another one of the areas where we have had very considerable technical and technological advances is in tracking people's movements. I am not very clear on how advanced we are on tracking their movements domestically but clearly we now know a lot about their movements across international borders. Is this a major infringement or potentially a major infringement to individual rights and liberties and privacy, or is it a minor matter? What is your view on this? Do we need more safeguards?

Dr Metcalfe: JUSTICE's view is that this is a very serious matter. I think a lot of passengers to the United States since 9/11 have perhaps not appreciated how much information the United States Government has required of them and that has been passed without their knowledge. There was a recent decision from the European Union in relation to the extent of the interference which was found to be disproportionate. Again, the European Union itself runs a number of very detailed databases, particularly for anyone entering the Schengen area, a great deal of information is gained. The Home Office is now rolling out its new border security network and anyone on a flight to the United Kingdom from any point in the world is now likely to find themselves flagged and cross-referenced with the information. There are various systems that are rolling out, but I think people fail to appreciate when they travel and, of course, international travel is becoming increasingly common, exactly how much information can be shared. I think this is a particular vulnerability because the regulation governing this is not merely what is governed by the United Kingdom, but is also governed by international agreements, in particular, agreements relating to counter-terrorism, and so states are far more willing to share private and personal sensitive information about travellers than they would be in relation to, say, their own citizens.

Dr Hosein: I am very grateful to you for raising this question because out of all the debates anywhere in the world, the least well-conducted debate is the debate about borders. As an international traveller there is nowhere on earth that you have less rights than at the border of another country, and we are not dealing with that issue. For example, this Government is moving forward on e-borders. I have spoken to senior members of every party and they have no idea what the plans are, we do not pay attention to the plans because we think it applies to other people. That is exactly why, in the United States, they are fingerprinting foreigners, the Americans do not seem to be very concerned, but if they started doing it to Americans, they would be very concerned; but we do not focus on the other. Passenger data transfers is a highly controversial issue that we have not had a debate on in this country which is unfortunate because what Governments are asking for is not just the passenger manifest, which is your name, your birth date and the country of your passport, they are asking for biographical data, such as your preferences, your previous travel patterns, the type of data that they then use to make decisions about you. The leading country in this is the United States, where it has been uncovered, despite laws preventing this from happening, there is an automated targeting programme that reviews all this data, much of which is unreliable—airlines admit this data is not reliable—they review this data using an argument that nobody understands and then flag you to say that you are a risk, or you are not a risk, or you are 80 per cent to be a risk, and you have no right to redress in any of these. This is exactly what is going on in this country; it is exactly what is going on in Europe.

Q267 ***Lord Peston:*** Are you saying this is a warning or, given the vast amount of data that we are talking about, is there anybody who could process that data, really on that scale, accurately? You are talking about enormous amounts of data and a lot of it is completely casual. I can see warning it as a threat but are you going further than that?

Dr Hosein: These systems are being developed. They probably do not work very well. You might have heard of situations in California about three months ago where the systems crashed and as a result they stopped admitting people at the airport. They had to reroute airplanes, they kept people in the terminal for 14 hours because they were terrified of letting potential terrorists through because they had become reliant on these systems. These systems are not reliable and that is why you have no legal rights in these systems because if you did you would be able to ask, "What information do you hold on me, may I correct it please, may I correct my profile?" You may not.

Q268 ***Lord Peston:*** But it is really misuse, often through incompetence, that you are warning about rather than a more totalitarian fear that we have at this stage, is that what you are saying? I do not know whether you have been across the Channel on Eurostar, but it is a really rather casual business. The idea that this is entering into a database as you are being waived through, I think seems to me to be slightly exaggerated. It is something one would worry about but I am surprised you are saying we are there now.

Dr Hosein: We are there now. Eurostar is a little bit more innocuous because there are no eating preferences logged in the databases.

Q269 ***Lord Peston:*** Oh, so, do not eat the food on the train?

Dr Hosein: That is it, indeed. But it does contain information such as who paid for your ticket, and that is sensitive to a lot of people. Is the company paying for your ticket? Is a prospective employer paying for your ticket? Is the Government paying for your ticket? The Americans are keeping this data for 40 years; that is their current plan. Why?

Q270 ***Lord Peston:*** Can I take you back to one other thing. Did you say—I was only half listening—that the fingerprints, say, mine that were taken in 1952 when I went to America for the first time to do research, the Americans store it for 100 years? So my fingerprints are still on record from all those years ago?
Dr Hosein: Yes, that is right.

Q271 ***Lord Rowlands:*** I would like to come back to more domestic issues. If these reports advocate new legislation to regulate CCTV cameras, I wonder if you could briefly outline what kind of legislation is required at the moment and how would it compare, for example, with the Information Commissioner's Code of Practice?
Mr Crossman: I am aware that for approximately 80 per cent of my time as Director of Policy at Liberty I am calling for fewer laws and the rest of the time when speaking about privacy I usually spend calling for more laws. So, you need to be able to justify why you are doing so. I think that CCTV is very under regulated. The Data Protection Act provides a regulatory framework. In the case of *Durrant*, which caused all sorts of consternation about the extent to which different CCTV systems were covered by the Data Protection Act, which itself is rather creaking at the seams and is rather outdated. New specific legislation covering CCTV is needed, which would be drawn very much on the ICO's guidance; the ICO provides very good guidance. It is very detailed about where, how and what is the justification for placement of individual CCTV systems; a very good idea. There is no reason why that cannot be in statute. The difference being, guidance is guidance, statute has the capability of enforcement. That would be the template on which I would base it and when I talk of enforcement, which is not something you generally do at Liberty to talk about bringing sanctions, but the ability for civil sanctions to be imposed upon authorities who fragrantly breach the requirements under the CCTV legislation, the possibility even of criminal sanction for people who intentionally misuse CCTV footage with the intention to cause harm to others. Basically, the Data Protection Act does not provide the perfect framework, it is a very long way from being the perfect framework. The ICO and also many local authorities, with the local government information unit guidance, have provided a very good basis. It is not a very big job to take that and put that into the basis of more formal statutory regulation.

Q272 ***Lord Rowlands:*** I do not know if you read the evidence that a senior police officer gave us a couple of weeks ago on CCTV. The impression that was left, on me anyway, was that it is incredible the way it has grown like Topsy and indeed, the vast majority of it is in the private sector and not the public sector. Do you think it is going to be feasible to try to construct a piece of statutory legislation that covers this now huge gamut of existing, let alone future, CCTV provisions? Can you explain to us the problems of even matching up one kind of system with another, in delivering useful evidence for a court case, for example. I would just like to know how you would manage legislatively to cover that whole world.
Mr Crossman: That does raise another separate issue which is that you can pass all the laws in the world but unless they are effectively enforced then it is not much use. The Information Commissioner's Office does very good work. They have tried as well as they can to provide appropriate guidance on CCTV. I think they are very much under funded and find it very difficult to do the job that they do. I do not see a significant problem in having an overarching piece of legislation that applies to both public and private sector.

Q273 ***Lord Rowlands:*** The legislation would apply to retail premises which have a camera?
Mr Crossman: That is exactly what the Data Protection Act does now. The point I might make about that is that there is an arguable case for a separate CCTV Commissioner.

Q274 ***Lord Lyell of Markyate:*** I agree with so much of what you say, but I think we are just overwhelmed with regulation and if every small shop has got to make an application to a local authority to have the CCTV in its shop –which really does not worry me one bit—I just think you are piling it on and think you should concentrate on other points. Can you tell us what benefit would come from this?
Mr Crossman: I do not see any fundamental change in the structure of the system. At the moment, if you operate a CCTV system, which falls under the Data Protection Act, you are supposed to register with the Information Commissioner's office. I think a lot of people do not, but they are supposed to. I am not saying that it should be any different, I am not saying that camera systems like private systems that do not look out and are not focused on different areas which currently fall out of the DPA, I am not suggesting that they should be brought in to CCTV legislation. Essentially, I am not saying that there should be any change in which cameras are governed, what I am saying is that there needs to be better regulation. In

fact, I think this would lead to far fewer cameras. The problem we have, particularly in terms of crime detection is that the systems we have are often very poor. I used to practice as a criminal lawyer and I know how poor some of these systems are for evidential purposes. I think fewer but better systems would be brought in by regulation. With fewer cameras, the footage they did have might be of better use in crime detection.

Q275 ***Lord Rowlands:*** Did I hear you say that you wanted a CCTV commissioner?
Mr Crossman: I think it is an idea.

Q276 ***Lord Rowlands:*** Normally, you are wanting to do away with Commissioners not create new ones.
Mr Crossman: I know I am. The reason I say that slightly guardedly is because I would be loathe to suggest anything that increases the resource burden on the Information Commissioner's Office who I believe is very much under-resourced. Given proper resourcing for his office, I do not see any reason why he cannot continue in the same way as he regulates the DPA, to regulate CCTV more generally. That is the reason why I suggested it, not loading any more work on him.
Dr Metcalfe: Just to reinforce very briefly the point made by Mr Crossman that you can have all the laws that you like but enforcement is key. What we find at the moment is that the Information Commissioner is struggling to cover both the public and private sectors. In particular, and this is a very simple point, the Information Commissioner has the power to audit a private company in relation to their data protection, for example, but they do not have any power to compel an audit. So they can request an audit and if the company agrees, the Information Commissioner can carry out the audit. If the company refuses, then the Information Commissioner cannot act. That seems to us to be a basic anomaly.
Dr Hosein: CCTV is a great example of public policy failure in the sense that we do not know how many cameras there are, we do not know how much they cost, we do not know how they are actually used, yet we keep on supporting them. I do not quite understand how that works. I do not understand how other countries can get by without CCTV cameras or focus on a specific environment. The Home Office report from last year said that on anecdotal evidence –and you probably heard this from the senior policeman you referred to earlier—80 per cent of the images are not of use. So why are we spending money on all these cameras? It does not add up in the end and I cannot figure it out. For example, my own council sent me an advertisement last month which said, "Oh, we are spending more money on public safety, we have invested £1 million in ten more cameras", and they say, "some of which will be focused on problem areas". Well, where are the rest going? And why is their entire policing budget going into CCTV? Does that local council know the evidence about CCTV? Has it questioned the effectiveness of CCTV? No, the politicians and policy makers grab budgets, throw them at CCTV because the public seems to want it and it seems to be the solution to a problem that they have not yet quite identified.

Q277 ***Chairman:*** Could I move on from CCTV to wider aspects of the Data Protection Act. Liberty's written evidence said that the Data Protection Act is not equipped to cope with mass data processing exercises because, for example, the requirement that processing should only take place for specified purposes is weak. Can you say how you think this weakness can be overcome and the working of the Act improved?
Mr Crossman: I know that time is an issue here so this subject is covered in a fair amount of detail in the report which I have handed to you, so I will be quite brief. The Data Protection Act is a piece of legislation based on the 1995 Directive, which was good for the time but is now showing the strain of not being able to deal with mass informational sharing, which ten years ago was pretty much unimaginable. It is not simply looking at the Data Protection Act, it is looking very much at the Information Commissioner's powers to take proactive action to ensure Data Protection compliance. But there are issues, both over implementation of the DPA, over, for example, the definition of personal data, where the UK seems to have not applied the definition of personal data which is contained in the Directive and enforced by many other countries, which allows data to be franchised out in a non-DPA compliant way. The Data Protection Act is not an enforcement or regulatory mechanism, it is an administrative mechanism. The way it is set up, it says, "This is how things will happen", but if they do not happen, there is not really much comeback. Something a little bit more robust is overdue.

Q278 ***Lord Lyell of Markyate:*** This is a very good paper by JUSTICE, if I may say so, particularly in explaining the role of the common law and the development of the law. But, how important do you think human rights legislation and European regulatory frameworks are in safeguarding United Kingdom citizens from the dangers of surveillance and data collection? How might this kind of regulation be improved? You point out that there are many more regulations in Europe, that they approach things differently. Can you explain it to us?

Dr Metcalfe: We cannot go the European route, we cannot rework much of our legal system. The European approach to personal identity is very different, they have the registration of names, for example, whereas under common law, you are free to call yourself any name that you choose so long as you do not commit fraud or deceive another person to obtain a benefit thereby. We are pretty much stuck with the common law tradition in the way we enact legislation and the way we interpret our legislation. The European Convention on Human Rights as an overarching framework is extremely important in providing a general principle –the general right to privacy—and that is very valuable. I would also say that European Union law is very helpful, in particular, the work of the European Data Commissioner in protecting the privacy rights of individuals in relation to the various information gathering powers that the European institutions have, particularly the European Commission, but obviously, more work needs to be done. There is very limited awareness—certainly at the public level but even among Government departments—of the very broad reach of European law into our domestic law, particularly as it relates to privacy. A very good example of this is the information-sharing agreement between law enforcement databases. It is now going to be possible for law enforcement data to be passed between European Union countries, on the basis of mutual recognition, which is that the information held on the police database will be available to other police forces throughout the European Union. The concern, of course, is that we have very strong data protection standards for the police database, relative to other European countries, but we cannot say with complete assurance that other European countries, particularly other accession countries, have quite the same standards, yet we are prepared to transfer that information.

Dr Hosein: I am not convinced—I am going to be slightly controversial—that the UK Information Commissioner has ever stopped a problematic surveillance programme in the way that his colleagues in Europe have. Children are fingerprinted in schools with the consent of the Information Commissioner in this country, yet in Ireland and Hong Kong, those practices were banned. The Greek Commissioner in the past has prevented his Government from fingerprinting visitors to the country, even during the Olympics, which was a high security event, and has forced the Government to remove information held on ID cards. The German Commissioners regularly force back Government proposals whether it is about collection of biometrics or advancing surveillance systems. I have not seen a similar level of activity in this country.

Q279 ***Viscount Bledisloe:*** To the layman, we seem to have an awful lot of Commissioners, we have an Information Commissioner, a Surveillance Commissioner, an Interception of Communications Commissioner, an Intelligence Services Commissioner and now you want a CCTV Commissioner. Is there any scope for a rationalisation or a centralisation of these functions and do they on top of that additional powers?

Mr Crossman: In answer to your first question, absolutely. I would get rid of the system of having separate offices for the Surveillance Commissioner, Interception of Communications and Intelligence Services Commissioners because it is unnecessary. The only reason there are three of them is because historically we have had these three bodies. We should get rid of the whole lot and have a single Commissioner responsible for the oversight of intrusive surveillance currently covered by RIPA. As I said with the CCTV Commissioner, that was merely a suggestion in relation to the current powers of the ICO. It is not about how many commissioners you have, it is about the powers that they have and the powers to act proactively. Responding slightly to what Mr Crossman said, the ICO acts within the remit of his powers. He does not actually have much in the way of power, so it is not about how many commissioners you have but ensuring that, especially against public bodies, that is where the difficulty often lies, it is easy to take action against the shopkeeper but it is a bit more difficult to take action against a Government department. Governments do not like franchising out powers to those who can take action against them. However, I think it is appropriate that certainly in the case of the ICO and for example the Identity Card Commissioner, who also lacks sufficient power in my view, that you have a small number of robust commissioners.

Q280 ***Viscount Bledisloe:*** As Dr Hosein has just pointed out to us, in other countries the Commissioner is prepared to take on the Government; why should not the Commissioner be prepared to do so in this country?

Mr Crossman: As I said, the Commissioner is a creature of statutes and the statute sets out the powers that he has, and he does not have enough now.

Q281 ***Viscount Bledisloe:*** They need wider powers?

Mr Crossman: Absolutely.

Dr Metcalfe: It is just a very simple suggestion in terms of rationalisation: you could actually scrap the Interception of Communications Commissioner, you could scrap the Surveillance Commissioner, if you have prior judicial authorisation. It is a slightly glib proposal, but if you think about it, the most important function of the Interception of Communications Commissioner and the Surveillance Commissioner should be the authorising of individual warrants. They do not have

the time to do that, but there is a large number of magistrates, a large number of judges in this country, who are perfectly able to make those kinds of decisions in relation to search warrants, injunctions and all the other measures that we ask them to authorise. Rather than overburden a single Interceptions of Communications Commissioner, why not have prior judicial authorisation of warrants and you would in fact by that stroke have much better, proper supervision of interception of communications for example.

Q282 ***Lord Morris of Aberavon:*** Is there not a danger on the other side of the coin of all the concentration in one office? With three, you might get somebody out of line, perhaps, who might pinpoint the danger. With everybody under one roof you will only hear one voice.
Mr Crossman: The trouble is that they operate absolutely independently of each other depending on which tunnel of RIPA you are talking about.

Q283 ***Lord Morris of Aberavon:*** But is there not strength in that?
Mr Crossman: No. Why is there any reason that the Surveillance Commissioner's Office should need to provide prior authorisation for non-urgent cases involving the police, but the intelligence services not be covered by exactly the same process because they are subject to the regime of another Commissioner, which is the Intelligence Services Commissioner? I do not know why. I am not saying this should happen, to take your point, if you had a statute which set up three commissioner's offices with very clear demarcation for justifiable purposes then, fine. But that is not what has happened. I was not around when RIPA was being proposed, but I imagine what happened was that there was a lot of stamping of feet and people saying, this is our remit, the statute must take this into account. There is no logical rhyme or reason why we have this incredibly Byzantine system.

Q284 ***Lord Rowlands:*** Privacy International produces these global "league tables" and this is for Dr Husein and I think we will move on with it. From the last table that we have had, we come out worse than Romania and on a par with Malaysia, China and Russia. It stretches some of our imaginations that that is the case. I just wonder how robust are such international comparisons?
Dr Hosein: That is a summary of a 1,200-page report that we released this year. We release every year a report on the privacy practices in currently 70 countries. There was only so much time over the Christmas break for me to create this map, so I limited it to 45 countries that we included in the analysis. It is the second year that we have included such an analysis comparing countries. On top of the 1,200-page report, this is also based on regular communications with privacy officials, parliamentary officials, around the world feeding us information about what is going on in their respective countries. The United Kingdom, for the second year running, has come out as the worst democracy for surveillance for all the reasons we have discussed so far, such as communications surveillance not authorised by independent magistrates, for instance; for the ID card in this country going well beyond the ID card of any other country on earth, perhaps on a par with Malaysia, I believe; no other country on earth is even considering doing mass-compelled finger-printing of its entire population, but this country is insisting up that; medical records being centralised in a single database made accessible widely across the Government services, that is not being considered in other countries; and as we have said already, the UK is home to more CCTVs than any other country around the world. What we found most interesting last year when we released the report was that a number of Governments held press conferences saying that we firmly disagree with the results from Privacy International. The Malaysian Foreign Minister was particularly adamant about his concerns with our work, yet when this Government was asked to comment on it they simply supported it. They said that our surveillance helps combat terrorism and crime.

Q285 ***Lord Rowlands:*** It implies that even with something like the rule of law—I am thinking of Romania, for example—am I to believe that we are worse than Romania?
Dr Hosein: For what it is worth, Eastern European countries have taken a very strong stance on privacy. They are realising that there are growth areas in this work and Romania is one of the countries leading. It is not to say that Romania is great and Greece scores very highly there too, it is not to say that any of these countries are great, it is just that they are less worse than the others. Last year, the leading countries were Canada and Germany, but they have fallen significantly because the Germans have moved towards the biometric ID card—but nothing close to what is happening here—and they started adopting EU law that they do not have adopt. And the Canadians have enforcement of their regulations.
Lord Rowlands: The way you do it, you have got these boxes and we are worse in some and not in others. The interesting one from the Constitution Committee's point of view is that we are in the worst possible box on constitutional protection, as opposed to statutory protection, where we are not in the worst box. What sort of constitutional protections do you think we need to get ourselves up from the bottom of your league tables?

Dr Hosein: I am conscious of the fact that I am not a lawyer and I am sitting before the Constitution Committee, so I might show my ignorance on this. Across Europe, not only do countries adhere to ECHR but they also have specific constitutional protections within their own constitutions. When they do not have specific protection, such as in Germany, where there is no explicit right to privacy under the German constitution, in 1983 the German Constitutional Court argued that the protection of privacy is part of Article 1's basic law, which is the protection of human dignity, so that created a fundamental right within German society. There is nothing in US or British law that compares closely to that.

Q286 ***Lord Rowlands:*** So, lack of a constitutional court brings us into this particular category, does it?
Dr Hosein: The lack of constitutional protections within this country, yes, absolutely.
Dr Metcalfe: If I might help. I think this goes back to the common law point that we have traditionally protected fundamental rights in this country in a pragmatic way, deciding not to regulate in those particular areas. In the 20th century—that has been overtaken and is now the 21st century—with the equally pragmatic instinct of government to gather as many useful tools as it can together with as much information as it can to do things which it sees as being in the public good. In doing so, the concern over the impact of these various useful tools has been lost. There is the issue of whether we are going to have a British bill of rights and that may provide, certainly if it were to model any other country—such as for example the Irish Constitution—you would expect to see a right to privacy in there.

Q287 ***Lord Rodgers of Quarry Bank:*** I absolutely do not feel oppressed. I have read all the details and how awful it is in this country compared with Greece and Romania and very much like Singapore. Am I deceived?
Dr Metcalfe: Yes.

Q288 ***Lord Rodgers of Quarry Bank:*** Am I deceived? I do not feel oppressed. Should you be saying to me, "you may not feel oppressed then you ought to be feeling oppressed"? I do not think most members of the public really feel oppressed at the moment.
Dr Metcalfe: Oppression is not the only harm. I would not describe ourselves as oppressed or that we dwell on the possibility of false consciousness. However, I think that the general public has a very poor appreciation of the extent to which information is held about them by a wide range of public and private bodies and I do not think they fully appreciate the implications. Indeed, do not think any of us fully appreciates the implications. I personally do not know how much information is stored about me and I cannot foresee how that might pan out in the future. The fact that Google keeps all my search engine inquiries for at least two years, for example, how do I know what the implications are of that? These things are unknowable. The information that a person might put in Facebook, for example, or their credit card transactions; I do not have a very good idea of how much information is stored about me and what companies are transferring information, which boxes I have not ticked. I think until you receive a letter from the Treasury explaining to you that your personal details have been lost in the post, and unfortunately your bank account details may now be made public, it is only at that point that you begin to appreciate the potential impact of the amount of information that we store.

Q289 ***Baroness O'Cathain:*** I think you have answered my question about whether we know how much is stored about us and whether it makes any difference. Is it important that the public should be informed and, if it is, whose responsibility is it to inform them? And tracking back to the question I asked you about donor opt-in, opt-out, how could you do it?
Dr Metcalfe: The first responsibility is on the person collecting the information, or the body or organisation collecting the information. There are certain obligations at the moment to inform the person in relation to data collection, but I think there is a case for making those obligations stronger and more clearly. I also think there is a very strong role for Government in making sure that the implications of data collection are far more clearly spelt out, and particularly the overall principle of transparency in Government that public bodies are much more transparent about the information that they gather.

Q290 ***Baroness O'Cathain:*** Can I just point two warning cones, one is small print that nobody ever reads and the second is trust in government and public bodies. So there are big antis about what you just said.
Dr Metcalfe: Yes, trust in public bodies, I completely take your point and I also take your point about the small print. However, trust in public bodies reinforces the case for strengthening the role of bodies such as the Information Commissioner; the independent regulatory bodies to make sure.

Q291 ***Viscount Bledisloe:*** Do you have any view as to the relative fact of privacy, which stems from public personal information processes in the public as against the private sector, or is perhaps the greatest risk the increasing interchange of information between the public and the private sector, and vice versa?

Dr Metcalfe: I would certainly agree with that last point and it is, of course, fair to say that the Government in the last resort has the most power to compel information from individuals. But I refer back to my earlier point about Google, which is an example of a private company which many people use on a daily basis to seek information and the amount of personal and sensitive information that can be gleaned from the inquiries that you make on a computer over the last two years are all held by one private company. I agree that the collection and storage of private information by the private sector is an incredibly important issue.

Chairman: Dr Metcalfe, can I thank you and Dr Hosein and Mr Crossman very warmly on behalf of the Committee for joining us this morning and for the evidence you have given. Thank you very much indeed.

WEDNESDAY 20 FEBRUARY 2008

Present	Bledisloe, V	Peston, L
	Goodlad, L (Chairman)	Quin, B
	Lyell of Markyate, L	Rodgers of Quarry Bank, L
	Morris of Aberavon, L	Rowlands, L
	Norton of Louth, L	Smith of Clifton, L
	O'Cathain, B	Woolf, L

Examination of Witnesses

Witnesses: Mr Philip Virgo, Secretary General, EURIM (the European Information Society Group), Mr Toby Stevens, Director, Enterprise Privacy Group, and Mr Mike Bradford, Director of Regulatory and Consumer Affairs, Experian on the Surveillance Inquiry, examined.

Q292 ***Chairman:*** Gentlemen, good morning. Thank you very much indeed for coming. Welcome to the Committee. My apologies for keeping you waiting for a bit. We are not being televised but we are being recorded, so could I ask you to state your names and organisations for the record?
Mr Stevens: Toby Stevens, Enterprise Privacy Group.
Mr Bradford: Mike Bradford, Experian.
Mr Virgo: Philip Virgo, EURIM.

Q293 ***Chairman:*** Thank you very much indeed. Would you, before we start questions, like to make an opening statement?
Mr Stevens: Very briefly. Thank you. My Lord Chairman, I am the Director of the Enterprise Privacy Group which is a think-tank for public authorities, private companies and academics to collaborate and resolve issues arising from the management of personal information. We meet regularly to develop shared intellectual property in the space which we then also share appropriately to inform the public debate. The opinions I give today are my own and do not necessarily reflect those of my group's member organisations.

Q294 ***Baroness O'Cathain:*** Could I ask how that is funded?
Mr Stevens: We are privately funded by member subscriptions.

Q295 ***Chairman:*** Thank you.
Mr Bradford: My Lord Chairman, I am Mike Bradford, my role within Experian is Director of Regulatory and Consumer Affairs, so my role is effectively to ensure that Experian complies with both the letter and the spirit of all data-related legislation, privacy and so on. Experian is a plc listed in the FTSE-100, employing 15,500 people across the globe. One of our principle activities is that of a credit bureau or credit reference agency but, more accurately, we provide private and public sector clients with data and solutions to enable them to build citizen or consumer relationships. We also do a lot of work with consumer groups and consumers directly to try to break down the concerns or myths they may have about the uses of personal data.
Mr Virgo: I am Philip Virgo, Secretary General of EURIM. EURIM brings together politicians, officials, industry to look at difficult policy issues that cross organisational boundaries. Originally it was, I suppose, a spin-off from the Parliamentary IT Committee but it was set up very much legally, financially and everything else separately, but it has a very heavy overlap of membership. I think our accounts are on the website, together with full details of our governance. It is a company limited by guarantee, so it is not a registered all-party group but in many respects it behaves as though it was.

Q296 ***Chairman:*** Apart from data security, how seriously you think the information technology industry and its customers take privacy and human rights issues? How do your organisations work to improve the awareness and behaviour of the industry and its customers in the development of information systems that collect and process individuals' data?
Mr Virgo: I am asked to lead on this. We discussed it outside. The main thing is that the IT industry and its customers are as confused about privacy and human rights issues as the whole of the rest of society, including policy-makers and Parliament. There is a great raft of pressures in the IT industry of "put your data on social networks", "give us your data" and so on, so there is one group which does not appear to value these things at all and about five million of the population have put things on to those websites that one would never dream of putting on if you were concerned about privacy, and then there are those who take the privacy and confidentiality of their customers extremely seriously, but every regulator in sight wants them to record every transaction or communication and make it available for posterity in case it is needed. We really do have an extremely

confused situation, where the IT industry is trying to meet the demands of those who are serious about trying to meet the needs of their customers, including government, regulators and everybody else, who are extremely confused as to what the priorities are and what they should be doing.

Mr Bradford: On a slightly different tack but nonetheless agreeing with my colleague, as one drills into organisations, the awareness of IT privacy issues, human rights issues, is very dependent on where that IT function sits within an organisation. If you look at some sectors, some immature organisations, you will still see the IT function and the IT specialist almost sitting in a silo. In more innovative businesses or more mature businesses, the most successful positioning of IT is very much allied to the business, so, as and when they are looking at systems development and so on, it is an integral part of what the business as a whole is doing, not just IT. Looking at certainly some big private sector organisations, you will find IT is very much a business facilitator and not merely a separate function in its own right.

Q297 ***Chairman:*** Is the industry interested in incorporating privacy-enhancing technologies in its products? Is it already doing so?

Mr Stevens: My Lord Chairman, firstly the commonly used expression "privacy-enhancing technologies" is one with which I am not entirely comfortable. I prefer to refer to "privacy-protecting technologies" since privacy enhancement suggests that you are being given something back that you were not necessarily entitled to in the first place. Certainly within our organisation we tend to talk more about privacy-protecting technologies. The industry is focused very hard on this. The problem that they often seem to stumble up against is the lack of a common framework, a common language, a common understanding of what the problems are and what the desired outcomes look like. The Engineering and Physical Science Research Council has kicked off some excellent work in that space to try to understand some of the more fundamental privacy issues faced by corporates, so there is a great deal of work happening. To date, most of the privacy-enhancing technology programmes that we have seen over recent years have failed, either due to lack of interoperability between those that roll them out or a lack of perceived consumer demand. That does not mean it is not there, but the consumers have failed to understand what it is they are being offered.

Mr Virgo: To build on that point, there are a lot of technologies about, some of which work, and they just have not been deployed for that reason. The bigger issue is not the technologies themselves. A really good secure technology is lethal if you now roll it out and give 400,000 people access to the data over it. The technologies are only there to support people processes. Basically, if you are going to give large numbers of people access to data over a secure technology, you are basically assuming that all the staff of the NHS are going to follow security processes rather better than the radio operators of the Wehrmacht and the Luftwaffe and the rest of it. I was trained as a Cold War radio operator and, basically, I would regard most of the systems, even if we were operating under military discipline, as unusable and insecure if you rolled out those numbers, and in a civilian environment the things have not been thought through. If you want security, it is either hierarchies or rings of trust, and it is broken up. Mass market systems and security are extremely difficult to reconcile.

Q298 ***Chairman:*** Perhaps I could ask Mr Stevens and Mr Virgo whether the training of information technology professionals includes consciousness of privacy considerations and what your organisations are doing towards that objective, if anything?

Mr Virgo: Speaking as a former Vice-Chairman of the Professional Board of the British Computer Society, it is included in the exams and the courses but I have to say that most of the students skip that section because there are not enough marks on it and it is worthy but boring. It is the issue of getting people to appreciate treating the data of your customers as though it is your own and building security right into the core of the system, so that you deal with us because we are more secure than they are down the road. Until that is part of the marketing requirement, then it will not be taken that seriously. That is a people issue, not an IT industry issue. It is an overall organisational thing. The industry responds to the priorities of its customers.

Q299 ***Lord Lyell of Markyate:*** Could I cut back to a question of which I am afraid you have not had notice but which is pretty fundamental: article 8 of the ECHR says that there should be protection of people's private and family life and so on. Are there some things which you could enumerate now which you would regard as utterly beyond the pale? If so, when being exercised by whom and in what circumstances? Such as, for example, "bugging". We have heard something about "smart dust"—I do not know whether it really exists but apparently it means you can listen to almost everybody's conversation by leaving this invisible stuff around—or there is hacking into people's personal computers to see what their interests and predilections might be in order to use them for some embarrassing purpose. What is beyond the pale in your view?

Mr Bradford: The two examples you have given there are perfect examples of subjectively what I would consider to be beyond the pale. When I look at the

way my own organisation uses data—and I guess my role in Experian is to act as the emotional and legal policeman for that—we will look very carefully at the legitimacy of what perhaps a client requires the data for. It is very much around what the Data Protection Act enables us to do. We will look at the public benefit element of that, which is not like the two examples you have given but is very much: "Is there a real citizen-centric benefit to that person having their data accessed?" or, the other way around—which is more the law enforcement end of things—"Is there a greater public benefit in an individual's data being accessed even though that individual may not have given their agreement to that?" I think the cut-off is somewhere in there.

Mr Stevens: Just to build on those comments, with which I completely agree, the two issues here that are very important to understand what is beyond the pale are, firstly, context. What for any one of us may seem a perfectly reasonable step, to another may seem totally unacceptable. The old example, of course, is that of a battered wife who has fled her husband: at that moment her new home address is an incredibly sensitive piece of personal information from her perspective. We go beyond the pale when we use disproportionate solutions in the handling of data; in other words, where for the individual concerned the use of that data is not proportionate to the problem or the social need.

Q300 ***Lord Peston:*** Are you saying that in the real world, to take the example of the battered wife, who gets a new credit card and the credit card will have her new address on it, that there is a way into the credit card system so that someone could access her address?

Mr Stevens: Unfortunately, it is the sin that dare not speak its name: insider fraud.

Q301 ***Lord Peston:*** I am still asking about the practice. A person who wanted to go and batter his wife has to find the insider and then go through this whole rigmarole. Is he not better off getting another wife and battering her? I mean, I really do think that a lot of the examples we are quoted do not seem to bear any resemblance to the real world. Can you give us an example? If I go into Sainsbury's and use my Visa card, which contains a lot of information, what process would then enable someone to get from my purchase to me? I would have thought the expense was massive.

Mr Bradford: My Lord Chairman, perhaps I might tackle that, bearing in mind my own business is very much part and parcel of providing clients with personal data. The fundamental in my own business, of any data-based organisation, is for us to be compliant and for us to retain consumer and client trust. We can only provide information that complies with the Data Protection Act. Fundamentally, unless that particular individual is aware of what their personal data may be used for and by whom, then any use of that data—and that could include, say, for example, using a store card and monitoring what your purchases are—if you had not previously been made aware that that was how you were going to have your data used would be a fundamental breach of the Act.

Lord Peston: That is really my point. The store would be looking at data of this sort to classify it and make it useful to them economically. Does the store have any interest in its individual clients?

Chairman: I am going to call Lady Quin next, because I think we have to move on, but I would just mention that my wife, two weeks ago, had a birthday card from Sainsbury's!

Q302 ***Baroness Quin:*** I am going to go back to something you started to address earlier on. It is about the factors which currently inhibit or encourage further development of PET—or perhaps I should say PPT—solutions, in particular what seems to me the difficulty of striking a balance between the need in large organisations to share information and at the same time build in fire walls and protection. In particular, are government procurement specifications sufficiently helpful in ensuring that data protection is designed into new systems?

Mr Virgo: It is before the procurement. It is the original concept of the system and the way in which it is designed and intended. The damage is done before the procurement takes place. There are assumptions made about the security of the people who are going to run the system which are not borne out in practice. One takes the very simple contrast: most of the Experians of this world vet all their staff and have rings of trust and the rest of it; but various government departments are tasked to meet quotas of recruits from various local communities. There is the example of the Immigration and Passport Service having to meet its quotas of recruitment in Croydon and that meant that all sorts of people were not vetted or checked and you have illegal immigrants ending up working within the system. That happens before anything has gone out to procurement, so, whatever you did in the procurement, you would actually have the "insiders" within the system. That is why I say secure technology operated by insecure people is lethal and, in that kind of example, you have the situation within the immigrant communities of forced marriages being policed and, if they try to escape, the extended relatives, who have access to the system for their job within the public sector, will help do the tracking and tracing and so on. There was the recent case of a tussle over a car-parking place in Asda resulting in the wife ringing her husband, who

rang a policeman friend, who then got the address of the pensioner, and they then went and threw a brick through his window and he died of a heart attack. No privacy-enhancing technology would address that kind of thing. The people processes are what you have to look at in that context.

Q303 ***Baroness O'Cathain:*** Does that mean that it could not ever be safe or that there is a sort of failure right at the beginning to specify correctly the whole system? Going straight on from that, is that not what has happened with government projects, and not only government projects but other big company projects, over the last ten years?
Mr Virgo: Exactly. It is the specification right at the very beginning. In government projects there is a systemic problem and the systemic problem is essentially that the policy is conceived by a set of advisors and a minister, it then starts gathering life and, on average—and I will not say this is statistically solid—between the policy being formed and the legislation going to the House there will be one change of officials, then between the primary legislation and the statutory instruments to implement it there will be two changes of minister and another change of officials, then you go through to the procurement. That churn means that whatever gets implemented is not the original policy and the specification gets compromised and corrupted along that process.
Mr Stevens: My Lord Chairman, may I add to that point—with which, again, I fully agree. For a corporate entity, security and privacy are the same thing: it is simply the nature of the data that they are handling. It is purely for the data subject that the privacy becomes a sensitive issue. I would certainly agree that government procurement does not reflect good privacy practice in general. This is not necessarily the fault of any one individual. We do see a problem that the cheapest way to implement transformational government objectives is to aggregate or "zipper" data into larger databases rather than taking the more complex but privacy protecting route of federated or compartmented databases—which, just as with a hole within a ship, will prevent leakage between the different areas—where we can manage the large user base without giving them access to everything.

Q304 ***Lord Peston:*** My question is about organisations promoting privacy impact assessments. I had assumed that most things like the Lord Chairman's wife getting a birthday card or the vouchers we get every month from Marks & Spencer, proportionate to how much we spend, and also from Tesco, were all done automatically by a computer and that no human beings were involved at all. Indeed, if you take the view, then you cannot have any privacy protection at all—after all, the person who posts the letters from Marks & Spencer can look through the whole list of letters and see some names. In promoting privacy impact assessments, I take it you are not asking for the moon.
Mr Bradford: Without knowing the ins and outs of that particular organisation, I would suspect the way that will work is that, at the time you opened up the relationship with that particular supplier, be it Sainsbury's or whoever, there will he what we call a "fair obtaining clause" that will tell you what your data may be used for, by whom and so on, and you will, strictly speaking, be given the ability to agree to that or potentially not to agree to it. If you decide, "Yes, I am happy for this to happen"—

Q305 ***Lord Peston:*** Who is "you" in this context?
Mr Bradford: As the consumer.

Q306 ***Lord Peston:*** It would never occur to the consumer. It never occurred to me until the Lord Chairman mentioned his wife's birthday card that these cases arise. One most wants to know about the organisation and its responsibilities. You cannot expect me every time I go shopping to do a privacy impact assessment.
Mr Bradford: The two are slightly disconnected. When you go into an organisation as a customer and you are going to transact or open a credit card or whatever you are going to do, there will be or should be a full explanation given to that consumer of what their data will be used for. One of the things may be: "We may use your data to contact you for future offers that may be of interest." That is, if you like, the obligation of certainly the organisation. As to a privacy impact assessment, to move on to that, perhaps I could draw again on my own role in my own organisation. Clearly we hold a lot of information which we have obtained fairly and lawfully within the meaning of the Data Protection Act. Consumers know their data is held within Experian and there are ways that we do that. When we come to look at designing a new product for a client to benefit a consumer, then we can only do with that data what the consumer has already been told. If, for example, the consumer has given their agreement that their data may be used, typically in the credit environment, for assessing a credit application, then the only way we can use that data is to help the client assess a credit application. We cannot take it out of there and develop, if you like, a birthday card list for a client so that all our wives and loved ones can get birthday cards. My job in the organisation is to make sure that every product that we design hits or meets that criteria, both the legal criteria of what we can and cannot legally do and, also, if you like, the reputation and emotional criteria

of what we should and should not be doing. That is the way it would work in my own organisation.

Q307 ***Lord Peston:*** Just to summarise, the answer to my question is yes.
Mr Bradford: If I could remember the question I would answer.

Q308 ***Lord Peston:*** The question is: Do you promote the use of privacy impact assessments?
Mr Bradford: Yes, we certainly do. We have to, yes.

Q309 ***Lord Lyell of Markyate:*** Some birthday cards may be legitimate but less welcome.
Mr Bradford: Absolutely.
Lord Lyell of Markyate: My next birthday will be 70 and I am expecting some letter or card from the DVLA at Swansea to tell me that I must now apply for an annual driving licence. That seems, albeit unhappy, to be legitimate.

Q310 ***Lord Morris of Aberavon:*** Could I ask about the ever-advancing development of the technical side of IT. How aware are the policy-makers and parliamentarians of this and of the social and citizenship issues of the surveillance society? How can we compare the awareness of policy-makers with that of other countries?
Mr Virgo: Having spent 25 years or so as piggy-in-the-middle in this area of trying to improve understanding between politicians and the IT industry, my honest answer is that the politicians understand the IT industry and the implications of technology rather better than the IT professionals understand politics and their responsibilities as professionals for trying to educate policy-makers about the potential implications of their technologies. It is not so much the theoretical technologies as to what might be possible, but what can actually be delivered with the technologies you have which are tested, which are working, and the people you have to deliver it. An awful lot of assumptions about technology cannot be delivered with the people, the time and the budgets you have. There was a meeting of very senior software engineers at what was then the Institute of Electrical Engineers. The conclusion was that the main protection for our privacy is that most of the surveillance technologies do not work and even those which do do not interoperate, and therefore an awful lot of the threats are theoretical rather than real.

Q311 ***Lord Norton of Louth:*** One of the issues you touched on earlier relates to the legislation process itself and whether it is fit for purpose in terms of its capacity to take into account privacy issues. Do you see any problems with the process as it presently operates?
Mr Virgo: There are a lot of problems. EURIM were heavily involved trying to do damage limitation on the original Regulation of Investigatory Powers Act, beginning with the Alison Halford case and IOCA review onwards, trying to get people to understand where each other was coming from. We then used that experience to try to help what became the scrutiny process for the Ofcom Bill and, in that, working with the bill team and the clerks of the House to try to do an exercise to identify the areas that were going to be relatively easy and the areas that were going to be difficult, so that they could plan and schedule what became the pre-consultation process before a joint committee of the Lords and the Commons, to make best use of the time to identify the things that were going to cause problems, so that the legislative process itself was relatively smooth. Observers have said that on a bill of that complexity it saved about 400 amendments. That bill would have had a couple of thousand and it went through with about 1400. Those really changed bells and whistles and made the implementation smoother; they did not really change anything that the officials had not already wanted to do and government wanted to do anyway. I can provide all sorts of documentation as to how that process worked—because I think it was a very good model and we spent a lot of time trying to make it happen—but there are limitations to it. I was consulting some of our parliamentary members, particularly one of the committee chairmen and he was saying, "Don't over-egg what you have achieved. All you did was make the process run smoother; you did not actually change anything."

Q312 ***Lord Morris of Aberavon:*** That was premised on there being pre-legislative scrutiny anyway.
Mr Virgo: Exactly.

Q313 ***Lord Norton of Louth:*** And that was exceptional.
Mr Virgo: It was, indeed.

Q314 ***Lord Norton of Louth:*** Is there anything that could be done on a more systematic basis and is there anything we can learn from overseas? In other words, is this a common problem?
Mr Virgo: It is, indeed, a common problem.
Mr Stevens: In the past five or six years, in particular, this space has been dominated by the tension between national security and citizen privacy, and national security in many bills, in my personal opinion, has been used to browbeat privacy concerns. Unfortunately, good privacy often results in much better data quality because it shows respect for the integrity and the handling of that data. We are seeing examples now of systems which are not delivering what was wished for because they were pushed through on a national security agenda when, in fact,

a citizen-centric, higher quality solution would have been achieved if we had looked at the bigger picture.

Q315 ***Lord Norton of Louth:*** How does one address that? Is it a procedural matter? Is it essentially a matter of awareness, so that you get that consistency, if you like the priority, given the—
Mr Virgo: It is awareness and prioritisation. The Belgian system, with its checks and balances and the rest of it, is extremely good but I think it is good because Belgium is a small but intensely federated country—more ministers per kilometre than anywhere else in the world. It also has this tradition of being occupied and the files being taken over by the Gestapo. That affects the reasoning why the Dutch and the Belgians particularly have much stronger and more solid and robust processes in this area, because of that legacy of mistrust.

Q316 ***Lord Norton of Louth:*** Is there anything we can learn from that in terms of process?
Mr Virgo: I do not think there is anything we can learn from the processes of other legislatures. In all honesty I would have to think about that rather more.
Mr Stevens: My Lord Chairman, may I add the example of Germany, where we have a written constitution that prevents the aggregating of citizen data at a federal level; where the government respects that to the point that they are able, in one example, to prevent the German state railway from issuing its own credit card. It was their own government that they stopped from doing that because it would have meant sending data overseas and aggregating it in a way that they were not comfortable with.

Q317 ***Lord Rowlands:*** Your last reply touches on the question I was about to ask you. We are a constitution committee—not just a public policy committee but a constitution committee. In a recent international survey of privacy laws right across the globe, we came out very negatively on constitutional safeguards. As three people who are heavily involved in all this movement information, et cetera, do you have any suggestions about what constitutional safeguards are required to bring this up to some better norm?
Mr Bradford: There is almost a flip side to what we are talking about. The word in the question "surveillance" society is something that concerns me. In our geographies, which are across Europe and globally, ironically, although the UK may be perceived as having weak constitutional protection around data, we need to be aware that by constantly referring to a surveillance society we are increasing the concerns of individuals—and I would argue, in many cases, potentially unnecessarily. At the end of the day, good privacy protection is designed to protect good citizens, and the very people that we end up not protecting by being almost over complex with the checks and balances we put in are the people we possibly would rather we did not try to protect. Without being too revolutionary about it, I think we need to be very careful that data breach reporting, uses of data, does not play to a mass gallery of almost privacy paranoia but plays to something that is a legitimate balance of privacy protection versus public interest. To go to that point specifically, I see how personal data are used across the EU. The EU is meant to be operating, for example, under one single European Data Protection Directive. It got 27 different interpretations of that Directive in 27 different countries. You could argue, looking at it commercially, rather than, say, from a strict privacy point of view: Is the best country that which interprets it in its most strict way? I would argue not. I would argue that if you look at the UK, which is constantly quoted by the World Bank from a credit perspective as balancing privacy interests with the ability to get credit—and you could argue is there an indebtedness issue and so on but we have hopefully parked that—then in the UK, which accounts for over 30 per cent of EU lending, we have a regulatory and commercial environment that allows consumers to use their data for their own benefit. I think the bigger challenge is around consumers starting to think—maybe the public sector: "What is my data being used for? Is it Big Brother?" I know that perhaps later we will be looking at ID cards and I think the bit we have to address is not so much process but one of trust and if consumers do not trust what their data is used for.

Q318 ***Lord Rowlands:*** You quoted the German example which was a constitutional safeguard. Are there any constitutional safeguards we should be considering?
Mr Stevens: My Lord Chairman, if I were able to propose a single safeguard it would be for an enhanced level of privacy controls over data where that is collected in a non consensual fashion. We pay taxes, therefore we expect the Treasury, the Revenue, to be able to gather information about fellow citizens to collect their taxes, so we cannot opt out of their databases. Nor can we take our business to another revenue if we do not like the one we are dealing with. Those organisations that are above that consent should be bound by a higher moral duty and subject to an enhanced level of inspection. The Cabinet Office and the CESG division of GCHQ provide the Manual of Protective Security and the various government memoranda/guidelines for protecting the security of data. It would be fascinating to see an equivalent function for personal data that is responsible for ensuring that the correct privacy impact assessments are carried out, and that is the

advocate for the citizen where non consensual data is processed.

Mr Virgo: There is an approach which we looked at but we never carried forward, not because we thought it was wrong but because the group concerned just stopped working. Essentially, we have far too many regulators, commissioners and so on in this area. We have an overload of governance and the effect is lack of confidence and no governance. The approach was, in fact, that all of these commissioners and all the rest of it should be replaced by a joint committee of both Houses. Given time pressures on the other Place, that would effectively mean it would be a committee of your Lordships who would have to be doing the work on it, but to have that governance open and transparent. At the moment, we have all sorts of officials who have the status of a chief constable and you then look and you find this is a functionary somewhere in the Home Office or the Ministry of Justice or what-have-you who has the "status of" and when you look at this from the point of view of, let us say, legal counsel to an American bank handling Arab and overseas clients in London, your reaction, as in the case of RIPA was, we move the files out of the UK. The dealers may be in the UK but the files and keys are sitting under Swiss or offshore legislation or they are split. "We do not trust this governance because we cannot understand it and our counsel tells us that it is different from what the minister said it was in the House."

Q319 ***Lord Lyell of Markyate:*** This is extraordinarily interesting. Could I just jog back to what Mr Stevens was saying about heavy-handed national security powers working against privacy-centric ideas. I think the point you were making was that if they had tried to be more privacy-centric, they would have got more useful data. Can you give an example or two of that?

Mr Stevens: To give a hypothetical example: obviously the polemic that has arisen from the national identity scheme has caused a great deal of debate over the past few years and this, in my opinion, is because the citizen cannot see the day-to-day benefit to them. National security/illegal immigration for most of us do not impact us on a day-to-day basis. As long as they are working they remain invisible. However, if we were to adopt the process used by many other countries to offer citizen-centric services to deliver true transformational government, to integrate business, I could, for example, enrol for a national identity card with a bank which happens to be part of the Government's broader scheme and then would willingly want to risk far more data with them because I would be able to get my own commercial value from that. The problem that we are looking at here is this lack of transparency in these schemes and where commerce has not been fully engaged from the start. Perhaps I could stress, My Lord Chairman, that is not a plea from my members in any way, shape or form but a personal opinion, and there would still be a lot of scope to explore schemes such as those in Hong Kong, Belgium, emerging in the likes of Canada, where they are taking this approach.

Q320 ***Lord Lyell of Markyate:*** Thank you. Is it possible to give a non hypothetical example? Because I am struggling.

Mr Stevens: Could I respond on that after please, My Lord Chairman.

Chairman: Yes.

Q321 ***Lord Woolf:*** What are your collective views of the efficiency of our current regulatory laws and other frameworks for limiting surveillance and protecting privacy, whether in the UK or in the EU?

Mr Virgo: I have with me a paper which was updated at my request for another purpose, particularly on our data retention requirements, because retained data is vulnerable data. We have retentions running from four days to a century under a whole raft of different legislative requirements, some going back to the First World War, others recent, and all of those retentions are, "We might need it because a regulator might need access" or "There might be statutory access" and that data is either properly managed (recycled and circulated so that it can be accessed) and therefore is vulnerable to abuse by those who are doing the management—and that is a very expensive process—or it is put into a long-lasting medium, down a secure coal mine, and is probably unreadable within a couple of years because computer operating systems have moved on, different microfiche readers and so on. There is a department of the University of London which is essentially a museum whose prime line of business is working with The National Archives rebuilding equipment to recover stuff from those obsolete technologies. It is a muddle and it is a confusion. It is because regulator upon regulator upon regulator says either "It is forbidden" or "It is mandatory" and has different requirements. They are never brought together.

Q322 ***Baroness O'Cathain:*** If you have these regulators, regulators, regulators, are they operating on a silo basis? Do they never talk to each other?

Mr Virgo: Some sporadically talk to each other.

Q323 ***Baroness O'Cathain:*** There is no requirement for them to talk to each other?

Mr Virgo: There is no requirement. The only organisation I have seen that has a coherent way of bringing them together is Lloyd's of London for the insurance regulators, which regularly runs courses and conferences for regulators, with extremely good

hospitality, and they all turn up because they meet each other and that is about the only occasion they do meet each other.

Q324 ***Baroness O'Cathain:*** Is there a need for an overarching regulator?
Mr Virgo: Yes.

Q325 ***Baroness O'Cathain:*** Rather than a joint committee of both Houses or the House of Lords Committee.
Mr Virgo: I would not say an overarching regulator because at that point you suddenly get hierarchies upon hierarchies upon hierarchies.

Q326 ***Baroness O'Cathain:*** Or silos.
Mr Virgo: You need a process that will bring about rationalisation and break open the silos over time.

Q327 ***Lord Woolf:*** It may be that you cannot answer what I was specifically putting to you: Do we need more legislation and, for an example, would you like to see changes in the Data Protection Act or the powers or the role of the Information Commissioner?
Mr Bradford: There are some very good things about the DPA but the one good thing in this context is that its design should be sufficiently dynamic to move forward with changing times, so if you look at the Data Protection Act it is virtually IT agnostic. It does not specify minimum requirements for this, that and the other, but it would put the onus on any organisation, be it public or private sector, to defend any data breach or whatever in line with the current best practice for information security technology, be it ISO or whatever. I think there are areas possibly within the Data Protection Act. In a commercial arena, basically it is our bible and everything we do with data must comply with that, and certainly on a quarterly basis we will be having discussions with Richard Thomas's office around what we are doing and what we are looking to do and so on. I think, though, in other sectors—and we have seen examples of this—there is far less clarity around what they can and cannot do and we have seen that leading to some rather unfortunate incidents where perhaps people do not think they can do something when they can. Whether it needs to be changed or whether there needs to be clarity around how it can be applied and interpreted, I would say it is the latter that could be addressed, not the actual legislation.

Q328 ***Lord Woolf:*** More information about what the legislation requires, is what you are saying?
Mr Bradford: Yes.

Q329 ***Lord Woolf:*** I think you are content with the legislation.
Mr Stevens: My Lord Chairman, to add to that, in my opinion the Data Protection Act, whilst it is a commendable piece of legislation, does of course operate as a business enabler to allow the transfer of data between organisations, individuals and nation states. The problem that we suffer from in the UK is an Information Commissioner's office that is not adequately resourced to keep up with the legislative burden being placed upon it. In particular, as a result, they have to remain focused on promoting data protection awareness rather than enforcing data protection because that requires such a great resource intensiveness for them. The majority of organisations in the private sector, if they were to choose to do so, could disregard most of its requirements, knowing that the outcome will probably be cheaper than the cost of compliance. Within the public sector we see many cases of non compliance resulting in no penalty at all for the individuals affected, where there is little point in transferring taxpayers' funds from one body to another in the form of a fine.
Mr Bradford: Perhaps I could pick up on a point which I think is very important. While the cost of non compliance in terms of censure may be potentially minimal, for a commercial organisation, especially a plc, to end up with a headline that says "There has been a data breach at Company X" is a phenomenal cost to the business. I do not think the deterrent need be on the small print; the deterrent is in the breach which will potentially be reported.
Mr Stevens: I would totally agree with that.

Q330 ***Lord Woolf:*** You have already identified the lack of resources for the commissioners. Do you need to see any changes with regard to their powers and their ability to have oversight? In particular, do you see the Regulation of Investigatory Powers Act as being effective in any way?
Mr Virgo: Yes. That is an extremely good point, because parts of the Regulation of Investigatory Powers Act are extremely good—the bits that are to do with the regulation of investigatory powers—and they need to be greatly strengthened. When the bill was going through, there was all sorts of stuff about the training and the codes of practice for those who were going to have the surveillance powers, and an awful lot of that training has never happened. Departments which did not train their staff in how to use the powers were supposedly going to lose the powers. That has never happened.

Q331 ***Lord Woolf:*** That is the enforcement of it.
Mr Virgo: It is the enforcement. As with the Information Commissioner, it is the enforcement powers and, particularly, the enforcement powers with regard to the public sector—because, as was said by my colleagues, the private sector is very concerned about its reputation; the public sector does not have

to be concerned about reputation because its customers do not have a choice.

Q332 ***Lord Woolf:*** I glean from your answers generally that there are problems but they are not with regard to the powers that legislation have given or prohibitions that the legislation has imposed.
Mr Virgo: When there is a breach of data protection. If I remember correctly, the Department of Transport civil servant who used his access to give names and addresses of cars outside Darley Oaks Farm to animal rights terrorists so they could then follow through had to be done for misprision in public office because nobody could find an alternative piece of legislation with suitable penalties. And if the individual had been a temp and not in public office, the penalties were derisory. There are issues to do with the penalties for breach which really do need to be brought through and enforced and implemented.

Q333 ***Lord Rowlands:*** Mr Virgo, I do not think I can let you get away with such a sweeping statement about the public sector that you have just made. There are staff in the NHS who are equally conscientious and as determined. You seem to give an impression that because you have a monopoly service of one kind you certainly do not care for your customers.
Mr Virgo: I am sorry.

Q334 ***Lord Rowlands:*** I think you should withdraw that—
Mr Virgo: I should indeed because it is the system and the way in which the system operates. You are absolutely right, some of those who are most concerned about data breaches are indeed those in the Health Service. I married into a medical family and they have very strong views on protecting the data of their patients, but they are protecting it, as they see it, against a system and the system is designed by people with particular mindsets. I do apologise for that impression because, you are absolutely right, it was a sweeping statement that I should not have made.

Q335 ***Lord Lyell of Markyate:*** What you are saying is very pertinent to the Regulatory Enforcement and Sanctions Bill which is going through Parliament. I personally am worried, and I have said it often in the Committee, that we are giving the power to every regulator—and that will go right down to local authority officials themselves—to impose fines. They are called civil penalties but they are effectively fines—which can be enormous but will often be automatic—but may be £1,000 and not variable. I am worried that we are going to see an awful lot of bullying and overkill. I can see that there are worries in data protection that they have not got enough, but there will not even be court surveillance, true court surveillance, if we go down this route. Has this crossed your desk as a problem?
Mr Virgo: This was the thing within the regulation of investigatory powers at a higher level, where industry wanted things to go through the courts and not through administrative procedures. That really is a major concern to industry that it wants things through the courts because that way it has a form of certainty that it does not have if it goes administratively.

Q336 ***Lord Lyell of Markyate:*** The Hampton Review by the Managing Director of Sainsbury's and the Macrory Report by Professor Macrory are leading in exactly the opposite direction, although we are told that it is all business friendly.
Mr Virgo: Those who are involved in information insurance and so on, who are looking for certainty, have one set of views, but this is not an area, I think, where you can say there is a single industry view. There are some things which are cheaper to do and there are others which are more confidence-enhancing. I have to say that certainly all of the meetings in which I have been involved have always been going down a route of: "These things should be open and transparent; they should not be behind closed doors administratively".

Q337 ***Baroness O'Cathain:*** My question regards the identification of individuals for marketing in commercial organisations and, indeed, for public sector services. These places—we have already dealt with some of them (credit cards et cetera)—involve identity management systems. Are adequate privacy and security safeguards incorporated in them and, if they are, do you think that can be transferred across to the current identity cards project in this country?
Mr Bradford: My Lord Chairman, may I start? If look at it from a commercial sector point of view, increasingly (and we saw this with our clients over the last probably six or seven years, in particular with Internet-based transactions) one of the first things a commercial organisation looking to transact with a consumer would want to do, especially remotely, is to verify, firstly, that there is a Mike Bradford that exists and, secondly, that the consumer at the other end of that telephone or Internet line is the Mike Bradford. Typically, in a commercial organisation what we call the authentication process, which is the, "Is this the Mike Bradford?", will be carried out with the agreement of that consumer who is looking, at that stage, to transact with this particular organisation. So, they will be informed at the point of transaction, firstly, that what we are going to do, if you are okay with it, is verify that you are who you claim to be (and it is very open, very transparent), and if at that point

they say, "No, we do not want you to do that", then maybe you go into paper proofs and the various other ways of doing things, but certainly in a commercial sector, unless it falls under one of two large but very limited pieces of legislation where there is a legislative requirement to provide data whether or not the consumer agrees to it, any identity management product will be operated with that agreement of the individual, and that is at the point of transaction usually.

Mr Virgo: The key point here, though, is in fact this one of informed choice, because far too many systems, even when there is a supposed choice, are: take it or leave it. In the public sector you have either got to give the information and it has got to be shared, or it is forbidden to be shared. There is not the element of choice which says, "If I give you more information, can you process my claim more quickly", and in the private sector very often there is a catch-all consent, or otherwise, and four pages of small print which may or may not be enforceable. I am trying to remember my business school law course and I cannot remember which legislation and case law applies—unfair clauses, and so on. On the actual issue of being able to choose to give more information in return for a discount voucher, or what have you, different organisations in the private sector deal with this differently. There are some which say, "Give us all this information. We will give you discounts. Oh, and by the way, we will not give it to anybody else except under a court order because we want you to do your transactions through us." They then guard that data, because it is giving them an advantage. There are others who try and collect the data and then sell it on. You need to have a choice as to which you are doing.

Chairman: Lord Peston. Can I make my traditional Chairman's appeal for brief replies, because time is marching on?

Q338 ***Lord Peston:*** Yes. What puzzles me, in a sense, this question, which is of fundamental importance, is the converse of the privacy question. The private sector seems to have cracked it to some degree. Certainly if I engage in online banking, I have to type in some numbers; if I engage in telephone banking I have to give them some numbers; if I go with my credit card now I have to put in some numbers and it seems to work very well, in the sense that I am identifying me as me and then it can all go ahead. What seems to be the mess is the public sector. This anticipates what Lady O'Cathain will go into in more detail. The public sector, having realised that people have to establish, for all sorts of purposes, "This is me", and then you think, let us have the equivalent, namely an identity card, has produced the most complex thing which no private sector firm would have engaged in anyway, apart from anything else, because of the sheer cost. A private sector firm would not have invented a scheme that would cost billions. Can you comment on that?

Mr Stevens: My Lord Chairman (and this also addresses the second part of my Lady's question earlier), I think the national identity scheme in particular has a very different fundamental requirement from a typical identity management scheme. If we treat credit cards and the very successful credit card networks as a scheme that we all know and trust, those systems tolerate a degree of fraud and it is factored into their business model. Fixing that final bit of fraud would be far too expensive, so it is far better to accept that that will happen. In a national identity scheme which is being used for national security purposes, that small bit of fraud could be the bit that causes the failure of the scheme by failing to identify the wrong individuals, and so on. I think there is a failure amongst some, and I stress some, policy-makers to understand the difference between, for example, authentication and identification and entitlement. A credit card proves that I am entitled to make this transaction and my PIN number authenticates that I am the genuine holder of this card, but the shopkeeper knows nothing more about me at this stage than my name, and that name is only on there so that I can pick up the correct card from the dresser in the morning and not accidentally come out with one of my wife's credit cards. It does not actually bear any relation to the transaction.

Q339 ***Lord Peston:*** Why could we not have a national identity card scheme exactly the same? Let us assume it starts as a voluntary scheme, so that anybody who wants to be able to say, "I am me", would simply voluntarily do it and he or she would get a PIN number?

Mr Virgo: Provided you accept that, like most of the identity cards around most of the world, it is a low-value, convenient residence card which simply you register with your council when you move in and you are going to pay your taxes and the rest of it, and when you move house it is a one-stop shop change of address. It is the expectations that have been added to that very basic concept that raise hackles.

Mr Bradford: My Lord Chairman, the other point about that as well—we touched on it earlier—is the more the citizen looks to use a card like that the greater the trust they must have in how it is being used, or how its data is used behind the scenes. I think that is another piece to crack.

Q340 ***Baroness O'Cathain:*** The point is, there are other countries that run identity cards, so all three of you must know in depth how those work. Are there any best practices that we could actually recommend

should be taken on board here, or is it like so much that we do in this country, we are gold-plating?
Mr Bradford: Maybe I can comment on that. If I look at it again, and I look at it from a commercial organisation's perspective, an identity card or an identity token that says, "I am the Mike Bradford", is only as good as the underlying checks and balances you can do before you issue that card. If I look at the UK private sector, unlike some of the EU countries or the States, we do not have access to the data layers that maybe the public sector have that would give you that certainty that you know that Mike Bradford with a national insurance number X, Y Z and a passport number of---. The card is only as good as the checks you can put into it. In the private sector and the public sector those checks would be, I think, far more robust than just one sector looking at it. That would be my point, I guess, that the efficacy of the card is dependent on the underlying data.
Mr Stevens: My Lord Chairman, there are a number changes that one could suggest, but for the sake of brevity if I may point the Committee at two areas. The first is to highlight the work that Microsoft has done in this space on the laws of identity by their chief architect. For example, one of those would be not using the same identifier for different purposes; so not using a national identity number for multiple applications, which would permit different agencies to zipper up data and build a broader view of the individual than they may be entitled to. The second one, to reflect my colleague's comment there, is rather than looking at other countries' identity schemes to look at the private sector and the trust that the likes, for example, of EBay have created in their reputational identity schemes, where a consumer can very quickly make a judgment about the individual that they are about to make a transaction with and decide whether it is safe or not. In my experience it works very well indeed. So, the reputational trust model to which Mr Bradford just referred might be one that would be fascinating in an identity scheme.

Q341 ***Baroness O'Cathain:*** Can I just ask a very quick supplementary. To your knowledge, are the Government's people who are looking at the future of identity cards in this country aware of the points that you have been making or even thinking along those lines?
Mr Bradford: Certainly in discussions we have had, Lord Chairman, they should be aware.

Q342 ***Baroness O'Cathain:*** But they are not necessarily buying into it?
Mr Bradford: I rest my case.
Mr Virgo: I would simply say that on Thursday we have yet another meeting which is basically trying to inform those looking at governments' identity management schemes, plural, of which the identity card is only one, about the experiences of the private sector around the world in dealing with other governments on identity management, because there are lots and lots of ways of doing it, both public and private sector, they have been around a very long time (thousands of years in fact), they have transitioned onto electronic media, and so on, but there is a great deal of it about and, yes, they are, indeed, looking at other parts of the world and other experiences, I think mainly because of the pressures they have been placed under.

Q343 ***Baroness O'Cathain:*** The Enterprise Privacy Group has been eager to develop a "business case" for privacy, which may be somewhat different from cases that could be developed on ethical, philosophical or social grounds. Can you explain the business case very briefly, because I know we are running out of time? Why do you think it is an important adjunct?
Mr Stevens: Very briefly, our hypothesis here, because it is early days in this piece of work, is that there is no duty upon a private company to offer privacy. They have a compliance duty for data protection, human rights and related laws. There may be a commercial imperative to manage their customers correctly, reduce fraud, protect security, but *per se* their shareholders have not tasked them with protecting privacy. We believe that privacy is, in fact, a secondary benefit to the consumer arising from good commercial practice, and that is the philosophy that we are now exploring in our work.

Q344 ***Baroness O'Cathain:*** Of course that is different when it comes to government?
Mr Stevens: Government, where we are particularly into non-consensual or monopolistic areas.

Q345 ***Baroness O'Cathain:*** And you are bound to be absolutely sure about privacy?
Mr Stevens: Yes, that is correct. So, that model at this stage is not the one we will explore; that is further down the line of our work.

Q346 ***Lord Rodgers of Quarry Bank:*** Experian says it has "a leadership position as the trusted steward of often sensitive information and we have an obligation to protect this". I assume, because I do not wholly understand the organisation, that they have to also take care of its shareholders. It is not a voluntary body; it is there to make money. I ask that really because, given that you collect and you process vast quantities of personal information of the kind we have been discussing, why should we have confidence in your stewardship or, whatever we might call it, custodianship?

Mr Bradford: It is certainly not something we would take as read. I think the expectation is because (a) of what we have to do with information and collect it from a data protection perspective, (b) the significant investment we make in compliance and in working with the Information Commissioner's office, (c) in the work that we actually do directly with consumers. We have a specific function whose job it is to work closely with the National Consumers Council, with Citizens Advice, and we have an area in our business with over 250 people whose job it is to work directly with consumers—not commercial businesses, not our commercial clients, but with consumers—and to try and help them understand the information we hold, why we hold it fairly and securely and any issues they may have with their data, how they can go around looking to protect that, in particular in the area of fraud, credit card fraud and victims of fraud. We advise our consumers, if that very unfortunate situation occurs, how they can manage their way through that. The very short answer, if I can abbreviate it, is that over a number of years we have tried to build this trust collateral externally, and it is something that will be in the commercial or public sector organisation. The big learning out of that is it takes a long time to build but it does not take long to lose, and I think, looking at ID cards and uses of ID cards, you have to build that reputational and trust collateral first before people have trust in doing business with you.

Q347 ***Viscount Bledisloe:*** Mr Bradford, it is in the interests of your organisation to collect as much information as it possibly can on people and to disseminate that to as large a number of companies as they can persuade to take it. Is that right?
Mr Bradford: Yes.

Q348 ***Viscount Bledisloe:*** I am not suggesting you are doing anything unethical. That is the main purpose.
Mr Bradford: With the agreement of the individuals.

Q349 ***Viscount Bledisloe:*** That is what I want to know.
Mr Bradford: It is not unilateral use of data.

Q350 ***Viscount Bledisloe:*** Does the individual actually know that information is being passed to you, does he have any opportunity to correct it or to comment on it and would he be happy that, in fact, this information about him is being disseminated worldwide?
Mr Bradford: I think we are back at the last point, but if I can give you a very quick working example of how a typical piece of Experian data would be used. When my colleague applies for a credit card, he goes to a credit card organisation and they will say at that point, "We will undertake a search with a credit reference agency", Experian or the two others in the UK, "(a) to check the validity of your application, to check who you say you are, and, if that application is successful, we will also share data on how you perform that account with other lenders." At that point there are a number of choices the individual can make. They can decide not to go ahead with the transaction, but from a consent perspective those three checks are considered in the UK to be a reasonable balance, if you lack a trade-off, for that person going forward with that transaction. At the end of the day, it actually helps that person get further credit lines because a good payer, if you like, when somebody else searches that individual, will be shown to have a good track record. So your agreement in that process is such that the data comes into Experian with your agreement; the next time you wish to make a credit application you have the same dialogue with another credit card issuer, who will then open up the Experian data. We are not sitting there unilaterally handing data out, the data is accessed at the point you apply for rental services with a third party organisation. In terms of correction, to go on to that point, Experian issues over one and a half million credit reports a year to consumers. They have a statutory right to ask the credit bureau for their credit report. We actually go further than that and facilitate that over the Internet, online and through partners. So, again, part of our consumer affairs function is to make sure that consumers know where their data is, how they can make sure it is accurate and how they can work with us if they find it is not accurate.

Q351 ***Viscount Bledisloe:*** You are saying that in some way, when I first take out my credit card, I have consented to them passing the information around, though I had no idea I was doing so, even though I happen to be a lawyer?
Mr Bradford: What will happen at that point, and again the Information Commissioner has been very involved in this and I believe EURIM have also commented recently, to use the analogy again, is that on every credit card application there are what are called fair obtaining clauses, and lenders are meant to give some problems to the wording, but legally these will be telling you exactly what your information may be used for, and they will be on those application forms. One thing we have to check and balance within Experian is, before we allow a lender access to our credit bureau, I will have sight of that lender's current credit application form to ensure that I am comfortable that it gives us, as the second party in the process, the ability to take that data. That is the process that it works on.

Q352 ***Viscount Bledisloe:*** Then I have a row with that card company because I think that they have overcharged me or something like that, I refuse to pay the outstanding balance and I stop using that card. When you are told, "Here is the money which he has not paid", do you find out? Are you told that it is because I have a legitimate complaint, or what I think is legitimate?
Mr Bradford: The safeguard for the consumer there, again, bearing in mind the priority we give to ensuring that consumers are aware that they can access their credit report, is that you could actually put a comment on your credit report, which any other lender will see subsequent to that. When it is sitting in a credit bureau the data is inert, no one is looking at it. The only time that that missed payment would be seen is if you were to make another credit application, and you have the right to put a comment against that to say, "I dispute this", or whatever wording you wanted put on there, because of a specific reason.

Q353 ***Viscount Bledisloe:*** I have to ask to see the report and then to put the comment on it?
Mr Bradford: Yes.
Viscount Bledisloe: I see.

Q354 ***Lord Lyell of Markyate:*** Experian's data, and you have got data on something like 460 million people, is supplied to a growing market in the use of personal information in a variety of businesses, no doubt very valuable. Can you describe the circumstances in which it is supplied in non-identifiable or aggregate form and those in which individuals remain identifiable? Do you try to influence your customers towards non-identifiability, where possible, in the interests of privacy protection?
Mr Bradford: My Lord Chairman, again with the example I have just given, I think, certainly for the majority of our business, it is based around the lender and a consumer looking at a very much consumer-based transaction. Clearly it is important in a case like that for the lender to be aware of that consumer's financial situation. The data may well be aggregated so that the lender gets a collective picture, but it will still relate to the individual. Examples where we would certainly not be looking to do that could be where we use aggregated and anonymised data at, say, postcode or postal sector level. An example of somebody perhaps looking to use that would be a major store looking to say, "Is this a catchment area with socio-economic groups A, B, C." So, we will do some geo-demographic profiling of that particular area, not using individual personal data, but using data that we have acquired from national census data, or whatever, that is in the public domain and that we can acquire. The difference between information that the consumer gives us for a credit application, which we certainly cannot use, and information which we can collect from within the general public domain, which we will then maybe model but you certainly cannot identify any individual, could be used, as I say, for store planning or something like that.

Q355 ***Lord Smith of Clifton:*** Could I follow that up? I would have thought that the ideal situation would be to take what is in the public domain about that postal code area and then read it across with the individuals you have in that area to see whether there is a mismatch or how far it equates?
Mr Bradford: It is an interesting point. I would love the answer to that question to be, yes. The reason we cannot is because the information that we hold at personal level is held for specific purposes; it is back to the fair obtaining clause. In other words, when I give my consumer data to Alliance and Leicester and it comes into Experian, I can only use that information for the reasons I agree to its use, and that will not potentially be for marketing purposes, it will not potentially be for putting with other data to form a view. The other thing as well: the UK shared credit information is governed by industry bodies, the British Bankers Association, the Council of Mortgage Lenders, which govern how data can be used, so Experian's credit bureau cannot unilaterally decide, "We have got these crown jewels and we are going to do something with it." It would obviously be good if we could, but we cannot, and that is both with privacy and commercial.

Q356 ***Lord Morris of Aberavon:*** If you have so much information stored, why, if I want to open a simple building society account, do I have physically to produce a fuel bill, a council tax bill repeatedly, time after time?
Mr Bradford: I cannot possibly comment on that particular building society.

Q357 ***Lord Morris of Aberavon:*** Every one. They say it is because of money laundering.
Mr Bradford: There are two things. This is a commercial answer, but I will give it nonetheless. We do provide online electronic systems that will enable that building society to comply with its money laundering regulation obligations. It is up to that organisation whether it chooses to do that. All I would say is that we have products that enable them to do it, but it is their call whether they use them. We have other organisations equally. I am sure if you walked into an Experian client to open a credit card, you would probably find that there would be online checks. I cannot speak for the individual lender, but clearly their own practices are such where they require paper proofs for that check.

Q358 ***Lord Morris of Aberavon:*** Take it from me, without exception, probably there have been half a dozen over the years that I have experienced.
Mr Bradford: You have obviously got a big commercial client opportunity.
Lord Morris of Aberavon: No. Nevertheless, the habit is the same.

Q359 ***Baroness O'Cathain:*** Is it not a feature particularly of a money laundering situation? Even if you have got an existing endowment policy, you still have to do it every two or three years and you have got to put in the same old thing when they know you very well and you have not touched the stuff. So it is money laundering, is it not?
Mr Bradford: It is money laundering, absolutely.

Q360 ***Lord Morris of Aberavon:*** I did say that. I qualified that when I asked my question.
Mr Bradford: Some organisations will still do that electronically.

Q361 ***Lord Rowlands:*** Is Experian interested in developing the market for more personal data for the public sector for either providing public services or for combating fraud in the public sector? If so, what implications are there for such developments?
Mr Bradford: My first observation would be perhaps sensitivity to the word "market".

Q362 ***Lord Rowlands:*** You are a purveyor of personal data.
Mr Bradford: "Market" suggests a unilateral and bilateral use of information without the consumer's agreement. I think we would be interested, we are interested, we are actively working with a number of government areas on how the public sector data and the private sector data can come together. As I say, because of commercial confidence I cannot talk about it here, but there are some significant government departments that we are in discussions with around potential products.

Q363 ***Lord Rowlands:*** That would be using data you have collected in the private sector in one way or another to assist a public service?
Mr Bradford: Yes, where we are allowed by regulation to use that data for the public sector, we will look to it to—

Q364 ***Lord Rowlands:*** Can you illustrate that first, because you have been making a very clear distinction all the way through your evidence that these are Chinese walls and there is information you must not transfer?
Mr Bradford: Yes, there is. There are two things that we cannot do with certain information. One we must do. One is to comply with whatever data protection obligation we have around that piece of data. If that piece of data were given to us on the back of credit risk assessments, we cannot then subsequently use it for something that is not a credit risk assessment with a public sector organisation unless that public sector organisation has a statutory right to access the information. For example, the Child Support Agency in its 1992 regulations actually lists the Credit Reference Agency as an organisation to which it has a statutory right to obtain data; so in that case we have to do it. In other cases, because the data Experian holds is obtained from commercial organisations, we can only use that data in line with what those commercial organisations allow us or licence us to do, if you like.

Q365 ***Lord Rowlands:*** I am not clear at all yet what sort of kind of data you can transfer to the public sector? Can you give an example?
Mr Bradford: There are two types of information Experian will hold, public information from electoral registers, to bankruptcies, to county court judgments to IVAs. There is data we will get from our commercial clients, which will be how somebody has performed on their credit card, dates of birth potentially. So, some data is our proprietary data, other data is data that we almost hold on licence, and it is the data we hold on licence that we have to be very careful how we use in other sectors.

Q366 ***Lord Rowlands:*** Do you think that the relationship between the private sector and the public sector handling people's data, the kind you are now describing, generates a new regulatory problem of any kind or raises issues of the question of the role of the Information Commissioner, et cetera?
Mr Bradford: I do not think it raises regulatory issues. I think possibly what it does lay itself open to is a more positive private/public sector discussion and dialogue around how data can be used in two respective areas. When you think about a lot of the commercial organisations out there, to take fraud as an example, fraud is not confined to the private sector; fraud is in the public sector as well, as I am sure you all well know, and the same people are liable to be the "won't pays". I think in legitimate public interest areas like that, there is a lot that the two sectors could work on together. I do not think it is a regulatory issue, I think it is an opportunity.

Q367 ***Lord Rowlands:*** The systems are always enough to ensure the citizens does not get rolled over on it?
Mr Bradford: That is what I guess we have been talking about. Famous last words, I would have confidence in my private sector system doing that, but equally, looking at the transfer of possible data

from private to public, we have to have that equal confidence that the things we have talked about, about knowledge of IT and so on, are as robust in the public sector. That is maybe where things come together.

Chairman: Mr Stevens, Mr Bradford and Mr Virgo, can I thank you very much on behalf of the Committee for joining us this morning and for the evidence you have given. The Committee will now go into private session to deliberate.

WEDNESDAY 27 FEBRUARY 2008

Present	Bledisloe, V	Peston, L
	Goodlad, L (Chairman)	Rodgers of Quarry Bank, L
	Lyell of Markyate, L	Rowlands, L
	Morris of Aberavon, L	Smith of Clifton, L
	Norton of Louth, L	Woolf, L
	O'Cathain, B	

Memorandum by the UK Computing Research Committee (UKCRC)

Executive Summary

1. There are few technical or commercial barriers to very widespread and potentially intrusive surveillance, data collection, and data retention.

2. It will be possible to search extremely large sets of such data cost-effectively, whether text, video or other formats, to identify individuals and correlate data.

3. It is extremely difficult to avoid large-scale leaks of data.

4. In view of the great difficulty of avoiding security breaches, our technical judgement is that it would be wise to:

- minimise the amount of personal data that is gathered, stored, and exchanged;
- minimise the storage period;
- minimise the number of people who have legitimate access and control the type of access allowed to minimise opportunity for abuse of trust;
- encrypt stored data using state-of-the-art cryptography;
- avoid connecting computers that contain large collections of personal data to the internet; and
- develop new systems to much higher technical standards than are routine in current commercial software.

Introduction and Technology Trends

5. The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society, the Institution of Engineering and Technology and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers from UK academia and industry

6. The technology for surveillance, data collection, data sharing and data analysis has advanced dramatically in the past decade or two, as a consequence of advances in information systems and sensors. UKCRC members have expert knowledge of current technologies and of technology trends. We have restricted our evidence to these technologies and their direct consequences in the areas covered by the Committee's Inquiry, as we do not claim particular expertise in constitutional affairs.

7. Thirty years ago, a large, mainframe computer with a 50MHz processor, and 512K of random access memory would have been enough to run a computing service for the whole of a medium-sized university. Today, most mobile telephones have a faster processor and more processing capacity than such a computer. The exponential trends in price/performance that brought this about will continue for many years; it is therefore reasonable to assume that there will be no technical or financial barriers to storing or processing surveillance records or other personal data.

The Growth in Surveillance and Data Collection

8. The range and quantity of surveillance and data collection by public and private organisations has increased hugely over the past decade, and surveillance is an integral part of modern life in the Western world. People have always watched each other—for reasons that range from the entirely benign to suspicion and fear—but with advances in Information and Communication Technology (ICT), the collection, processing, and transfer of large amounts of data has become vastly more efficient. Surveillance has become deeply embedded in government and business processes, "massive surveillance systems [. . .] now underpin modern existence".[1] The Government are currently considering changing the law so that intercept evidence is allowable in court.

9. UK government has embraced technology and the surveillance it affords with particular vigour. The UK is the country with the largest number of CCTV cameras. Government projects to establish and link national databases on its citizens abound: Connecting for Health (patient records), the National Identity Register (incorporating identity and biometric data), and the Children's Database are three high-profile examples.

10. Businesses also collect, utilize and share data an ever-increasing amount of personal and behavioural data on their customers. Many provide their customers with incentives in return for providing personal data, or consenting to collection of data on their behaviour. There is an increasing trend to collect, aggregate and trade such data without customers' awareness and consent, especially in online environments.[2] The general justification is, again, improved efficiency and effectiveness, and the ability to develop improved services or target them more carefully at those who are interested.

11. The justification for these developments is made in terms of benefits for individuals and society, and improved effectiveness and efficiency of key public and private sector services.

12. Many public and private sector surveillance schemes may fulfil their intended purpose, and deliver real or perceived benefits to individuals and/or society but reliable evidence on benefits to individuals and society is currently hard to find. There currently is little interest from government in committing resources to the evaluation of existing surveillance technology. The few studies that do exist tend to raise serious points as to whether the schemes do meet the stated goals.[3]

13. Similarly, few companies are prepared to reveal to what extent personal data delivers benefits to customers, as opposed to improving the companies' profitability (eg by prioritising high-value customers, refusing service to those with a high risk profile). Once collected, commercial data is available for use by the state.

Implications for the Future

14. Companies such as Google and Experian have shown that aggregated personal data has a commercial value. With data storage costing very little, the commercial balance has already moved in favour of retaining data rather than reusing the storage media. Costs will continue to fall, so it is reasonable to assume that the amount of data that is retained will grow rapidly.

15. The Royal Academy of Engineering's recent report[4] describes the current and forecast technologies for surveillance and data processing, and the dilemmas that arise because these technologies are disruptive: they change the relationships between individuals and the State, companies and other individuals in ways that can be either beneficial or damaging or both. The report shows that the same technology is capable of affecting different individuals, or different groups, in very different ways. As one example, the ability to tell where someone is might be helpful to parents responsible for school-age children, but very damaging to an adult trying to escape an abusive relationship.

16. The technology trends mean that it is likely that many forms of surveillance and other personal data[5] will be collected and stored. It will become increasingly easy to search and correlate these data sources (for example, to search large amounts of video data to locate pictures that include specific individuals). In our

[1] Surveillance Studies Network (2006): A Report on the Surveillance Society for the Information Commissioner (Full Report), edited by David Murakami Wood. http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx

[2] Information Commissioner's Office (2006): What Price Privacy? The unlawful trade in confidential personal information.

[3] See, for instance, the only major study on CCTV and crime reduction: M. Gill & A. Spriggs (2005): Assessing the Impact of CCTV. Home Office Research Development and Statistics Directorate, 43.

[4] Dilemmas of Privacy and Surveillance: challenges of technological change. March 2007. Available online at www.raeng.org.uk/policy/reports/default.htm.

[5] For example, time-stamped video footage; mobile phone location data; records of phone calls made and received; location data from radio frequency ID (RFID) attached to clothes and other goods; internet search records and web-sites visited; purchase history from the use of the internet, credit cards, store cards and ID card; medical records from every contact with a health professional or prescription; fingerprints; retina scans; facial geometry; gait; voice analysis; travel records from tickets and Oyster cards or equivalent; vehicle movements from automatic number-plate recognition; emails; postings on web-sites; and much more.

opinion, it would be reasonable for the Select Committee to assume that no aspect of any individual's life will be wholly private in future, unless effective measures are introduced to limit the use of the technology that is available now or that will be available in future.

17. The fact that a growing amount of data will be stored, potentially for a very long time, and that it will become possible to search this data very efficiently,[6] raises complex issues that have not yet been debated fully in public. All surveillance changes the balance of power between the watcher and the watched, so the increasing collection and sharing of data by public-sector agencies self-evidently has constitutional implications. Whether these changes will be beneficial is hard to judge, because the affects might only become apparent after many years and because, with any changes, there will be some individuals and groups who benefit and some who are harmed.

18. No collection of data is 100% secure. There is a growing list of mistakes and unintended outcomes, which have implications for individual citizens' liberty, privacy and life chances. When this happens, individuals usually find it difficult to put the record straight, or obtain compensation or redress. Despite the Data Protection Act and FSA regulations, there are almost daily reports on data leakage because of lost laptops, decommissioned hard disks, insufficient controls on database systems. There is also unlawful export and trade of personal data,[7] and existing penalties have not made a significant impact.

19. What is perhaps even more worrying is the probability of major criminal misuse of information obtained illicitly from inadequately secure databases, for example for purposes of financial fraud. One evident danger is that of stolen surveillance data being used, in conjunction with stolen credit card numbers, to enable identity theft and financial fraud on a hitherto undreamed of scale. (Already there are numerous examples of criminals obtaining credit card information relating to very large numbers of individuals, almost 50 million in the case of TJX, owner of the TKMaxx chain in the UK).[8]

20. Much personal data, for example, audit and banking data and the results of clinical trials, are required by law to be kept for a certain period. Such data could be encrypted to ensure that they cannot be used for purposes other than those for which the law requires them to be retained.

21. It is important that security is taken very seriously when new systems are developed, and that the strongest security policies are adopted and implemented. Commercial software is not secure, as the many examples of hacking, virus infections and trojan software demonstrate each week. Yet few public-sector developments, other than those involving military or equivalent security, plan or budget for adequate security of personal data or for adequate remedial action when security breaches occur.

22. It seems that project leaders do not understand their responsibilities for protecting individual privacy; in recent oral evidence to the Commons Health Committee on the Electronic Patient Record (EPR), Richard Granger, head of Connecting for Health, referred to some critics of the EPR as "privacy fascists". Other Government ministers have repeatedly said that "if you have nothing to hide, you have nothing to fear", yet most people will have some circumstances that they legitimately need to keep private, at some time in their lives. Obvious examples include HIV status, mental illness, and traumas such as rape. Even one's home address may need to be kept private, eg if one works for an animal testing laboratory. It is hard to predict what personal information may make someone the target of prejudice, as the attacks on the home of a paediatrician showed some years ago, as the result of an apparent confusion with "paedophile".

23. In view of the great difficulty of avoiding security breaches, our technical judgement is that it would be wise to:

- minimise the amount of personal data that is gathered, stored, and exchanged;
- minimise the storage period and use state-of-the-art methods to destroy (or render inaccessible) all copies of the data, including archived copies, at the end of the retention period;
- minimise the number of people who have legitimate access and control the type of access allowed to minimise opportunity for abuse of trust;
- encrypt stored data using state-of-the-art cryptography;
- avoid connecting computers that contain large collections of personal data to the internet; and
- develop new systems to much higher technical standards than are routine in current commercial software.

[6] The Royal Academy of Engineering report referenced above explains that it will become possible to search enormous amounts of historic data to discover what an individual was doing, and where, at any point in previous years. They capture this idea in Professor Andy Hopper's memorable phrase "Googling space-time".

[7] Information Commissioner's Office (2006): What Price Privacy? The unlawful trade in confidential personal information.

[8] Boston Globe (29 March 2007): TJX data breach is called the biggest ever.

24. UKCRC would be pleased to provide additional evidence, orally or in writing, on any of the points mentioned above.

June 2007

Examination of Witnesses

Witnesses: Professor Angela Sasse, UK Computing Research Committee, Professor Martyn Thomas, independent consultant and UK Computing Research Committee and Dr Ian Forbes, Director, fig one Consultancy, examined.

Q368 ***Chairman:*** Dr Forbes, Professor Thomas, Professor Sasse may I welcome you to the Committee and thank you very much for coming. We are being recorded, but not televised, so could I please ask you to state your names and organisations for the record?
Dr Forbes: My name is Ian Forbes and I am a consultant with fig one Consultancy and I am representing the Royal Academy of Engineering.
Professor Thomas: I am Martyn Thomas. I am an independent consultant software engineer. I was on the Royal Academy of Engineering Study Team and I also, with Professor Sasse, submitted the evidence from UKCRC.
Professor Sasse: My name is Angela Sasse. I am a professor at University College London and I am representing UKCRC.

Q369 ***Chairman:*** Before we proceed to questions, would any or all of you like to make a preliminary opening statement?
Dr Forbes: I would not mind doing that. It would be on the basis of the report of the Academy and the organising principle of that report is that protecting privacy, achieving greater levels of security and maximising utility will always generate dilemmas for individuals, governments and organisations. The development and use of technologies leading to a so-called "surveillance society" are associated with a wide range of dilemmas. Nevertheless, efforts to strike satisfactory balances are essential and can be achieved and be successful. The costs of not recognising and addressing these dilemmas include threats to, and a decline in public trust in some of these areas, inefficient allocation of resources and avoidable failures.

Q370 ***Chairman:*** Thank you very much. Perhaps I could start by asking about the UKCRC's written evidence which says " . . . no aspect of any individual's life will be wholly private in future, unless effective measures are introduced to limit the use of the technology that is available now or . . . in future". Could I ask whether such limits would be most appropriately placed on data collection, processing or the uses to which the data are put?
Professor Sasse: It is all three, but the emphasis has to be on collection. Once you have collected the data it takes resources and it takes effort and know-how to protect it and those mechanisms might always fail, particularly when there is mission creep; when there are competing demands, those safeguards may turn out to be inadequate. Also, once you have data collected, development of technology may mean that things you did not think were possible at the time when you collected them, can be done in the future. For instance, when the DNA database was set up, the possibility of familial screening did not exist.

Q371 ***Chairman:*** What kind of effective measures do you envisage and would they require legislation?
Professor Thomas: If I may, I would just like to add a couple of things to what Angela has said. One of the problems of collecting substantial amounts of data and then retaining it for a period is that you can carry out all sorts of correlations between data that were never envisaged before and that can reveal all sorts of aspects of individuals' lives which probably were not apparent to them at the time when they gave consent, if they ever did, for that data to be collected. Therefore retaining data, and in particular sharing data so that it can be correlated, undermines the principle of informed consent. On the sort of safeguards that could be put in place, it is quite hard. Enforcing the real letter of the Data Protection Act—requiring that only the minimal amount of data is collected for the purpose for which that data has been said to be collected—would have a profound effect and it clearly is not happening at the moment. There are just trivial examples, like the way that the Oyster card is collecting all sorts of data about people's travel patterns, which are not really necessary in order to carry out the functionality of providing a pre-payment card for travel. You can see many, many examples where, for example, people's names and addresses are collected when in fact all you need to do is to accredit them to be able to carry out some activity. That creates the fundamental privacy issue, because now you have identifiable personal data whereas previously you had data which it would have been a bit more laborious to turn into identifiable personal data. Two issues there really: one is restriction on collection and one is restriction of further processing and retention.

Q372 ***Lord Peston:*** Wearing my former professorial hat, what you are saying seems to me to make life very difficult for social scientists who have always had to get by on data not usually collected for them. What

you are suggesting is actually stopping them using this data. Most of us who have done research in fields happen to say "Ah, but I could use that data and correlate it with that data and then I might get some results". For most of my research lifetime, the idea that I would have to be involved at the beginning and get permission and all of that, would make social science nearly impossible it seems to me. To take your theme of travel patterns, there are social scientists generally interested in research into travel patterns and to be told that there is data, but because it was not collected for that purpose they cannot have it . . . I would fight like mad. I put it to you: do we not have responsibilities as scientists in the social area to fight that and not accept it?
Professor Thomas: There are some fundamental principles that need to be addressed. One is the principle of informed consent and the other is the issue of identification.

Q373 ***Lord Peston:*** The latter I accept, but the informed consent . . . If I am told that I cannot do research in this area because I did not get informed consent in the first place from several of the individuals who are in there and who will not be identified so I cannot do the research. I feel that that is incredibly anti social scientist.
Professor Thomas: But the two are linked; if you cannot identify the individuals, then you do not need the consent because it is not personal data.
Professor Sasse: The DPA only covers personal data.

Q374 ***Lord Peston:*** So as long as the data is aggregated, are you saying you would never ask for informed consent?
Professor Thomas: Ideally.

Q375 ***Lord Peston:*** Supposing I was to say on my Oyster card that I do not give consent when I buy my Oyster card. You are not suggesting that that should be how it works, are you?
Professor Thomas: No. What I am suggesting is that you could try to devise a way of setting up an Oyster card scheme that does not identify the individual. My Oyster card is not easily identified to me because I have never registered it and I have only ever topped it up with cash. It could be correlated with my mobile phone records.
Lord Peston: How is your terrorism activity going on?

Q376 ***Baroness O'Cathain:*** I was very interested in the point about the mission creep implications of all this. Of course, whereas you are right constitutionally about informed consent, et cetera, there seems to be now an overwhelming and overriding consideration due to terrorism and the so-called war on terrorism. At the base of all of this now is that the surveillance society equals our ability to stop crime or to avoid terrorist attacks, so how can you justify not collecting it?
Professor Sasse: I am sorry but I have sat in on quite a few debates where terrorism experts have responded to that question and their response has been that, no, the surveillance society does not prevent terrorism. Whether that has been in the discussion surrounding the national identity register or similar acts, it is basically a tempting but erroneous assumption that just because you can identify people this enables all sorts of security features and subversions.

Q377 ***Baroness O'Cathain:*** But the criminals involved in the bombings on the Tube were identified as a result of closed circuit television cameras; those people were identified by closed circuit television cameras.
Professor Sasse: Yes, they were identified and we are not saying there should be no closed circuit television anywhere. What we are discussing here is a proper legal framework that governs how that information is being used, who can use it, for what purpose, how long it is being kept and so on. Of course, you would want to be able to look at it for many crimes but does that mean that CCTV footage should be kept forever, and should be used for fishing expeditions as opposed to targeted investigations of actual crimes?
Professor Thomas: If I may just add a quick point, it is an easy mistake to make, but a dangerous mistake to make, to assume because certain data is available and it was used to detect few crimes, that therefore it was necessary to collect it, or that collecting it was proportionate, that it was actually more beneficial to have it than the damage that was done by collecting that data overall. If those particular terrorist bombers had not been picked up on CCTV, they would have been found by other means. They were not setting out to conceal their identities.

Q378 ***Lord Morris of Aberavon:*** May I come back to My Lord Chairman's question? What effective measures are contemplated to limit the use of technology in the future? As I understand it from Professor Thomas's answer, there is ample material in the Data Protection Act but it is not sufficiently enforced or not appropriately enforced. Is that the position? Is legislation needed?
Professor Thomas: I believe that strengthening the Information Commissioner's Office so that he has more resources to enforce the Act would be extremely beneficial. Giving him the ability to require that audit activity be undertaken—requiring, for example, that a company's auditors reported on compliance with the Data Protection Act—that could be very powerful because it would extend the ICO's reach and it would provide an independent check on

whether the DPA was being followed. The people who are most able to protect privacy are the people who are collecting the data and therefore shifting the burden of liability firmly onto those people would have a profound effect. If, for example, there were a statutory requirement to inform data subjects, whose data had been inappropriately accessed or lost, of that event that would be quite a powerful incentive to people not to lose data. If it had to be accompanied by a statutory flat rate of compensation, even at the level of £20, suddenly those databases start to have a significant financial value. A £20 individual compensation would have meant that the HMRC data, for example, was worth half a billion pounds and if you have a database worth half a billion pounds on a couple of CDs in your hand, you do not put it in the internal mail.

Q379 ***Lord Woolf:*** Is the real answer to what you have just said not that it is worth that amount of money but that there is a penalty of that amount of money and that penalty and the value do not necessarily coincide and the penalty in fact in what you are talking about would be totally disproportionate?
Professor Thomas: No, because it was unnecessary to ship that entire database and therefore what a flat rate penalty would do would be to cause people to think how many individuals' data they need to put at risk in order to be able to carry out this particular piece of processing.
Professor Sasse: The National Audit Office did not ask for the entire database, they asked for a subset of data and they would have been quite happy to receive them in a format that was not so risky. However, somebody at HMRC, or several people at HMRC, decided that the amount of money the contractor demanded for reducing the database and making it less risky, they made a judgment, was not worth it and the amount has not been revealed. I do not know what that amount of money was, but clearly it was a completely wrong judgment because that amount of money was not in proportion to the risk for all the people whose data was on that disk.

Q380 ***Lord Woolf:*** That is surely the thing. All these matters are cases where judgments and balance have to coincide. All I was questioning was that you do not improve the process of making a judgment by imposing disproportionate penalties. Now there may be conduct which is wrong, but to put a disproportionate penalty, especially when the disproportion is one which means it could never actually be enforced because the cost of enforcing it would be so colossal that it was unlikely, does not necessarily achieve the object you want to achieve.
Professor Sasse: I would argue that the current penalties that the Information Commissioner's Office can hand out are really completely disproportionately small.

Q381 ***Lord Woolf:*** That does not answer the point; that does not help.
Professor Sasse: Like Martyn, I would actually say that there should be a flat rate. It would have an incredibly good pedagogical effect on the people who are handling the data. I am an expert on human factors and security and I look at corporate organisations when things go wrong, why they go wrong. The key problem is really that our ability to assess risks associated with information technology with electronic data has not kept up, it has not developed in the same way as we are able to read risks in the physical world and even there, human beings are not terribly good at it. The people who are handling the amounts of data, because they are in contact with them every day, are utterly blasé about the risks associated with the data and the value and they have no understanding, I can assure you from my research, about the impact that that disclosure or leaking of those data has on the lives of the individuals who are affected by this leakage. Given that it is Government handling their own citizens' data, that is something that has to change. The Government have a duty of care.

Q382 ***Lord Lyell of Markyate:*** That moves us on to the second question where UKCRC's evidence says "There currently is little interest from government in committing resources to the evaluation of existing surveillance technology". I take what you have just said to be wrapped up in the idea of evaluation. What kind of technologies should be evaluated and who ought to carry out the evaluation?
Professor Sasse: The one area where we have had an evaluation after almost 15 years of deployment has been CCTV and it was evaluated in that case by criminologists and their conclusion was that the benefits of it were not proportionate, it meant that the claims the Government had made about the impact it had on crime prevention did not hold up to scrutiny and that certainly it was not in proportion to the amount of money that had been spent on it.

Q383 ***Lord Lyell of Markyate:*** Many of us feel that is counterintuitive. What do you think?
Professor Sasse: Many things in science turn out to be counterintuitive, but really it is fair to say that science currently is an inter-disciplinary area, how you use economic knowledge together with knowledge about social science, criminology; it is a very inter-disciplinary area. You need to agree on how you are measuring the cost of these various factors, of the impact it has on individuals, of the impact it has on

victims of crime, and you need to look very carefully at how much money you are actually spending on collecting information and keeping it secure.

Q384 ***Lord Lyell of Markyate:*** So my question is: who ought to carry that out?
Professor Sasse: My view is that we have the expertise in the UK, but certainly the Information Commissioner's Office has legal expertise and the technical expertise to some degree. The National Audit Office has expertise in this area and CSG of course has a lot of expertise when it comes to how we should value the risks when it comes to criminal or terrorist activity. In my view the problem is that very often when they do investigations they are not properly independent. The reports have to be agreed with the departments who commission them and if you make the effort to read the full report and compare it to the summary, you can see that things are . . . I will leave it there. A certain amount of pressure seems to be exerted to make it sound better than it actually is, or make it sound less bad than it actually is and certainly, if I compare it with other European countries, I do not feel these agencies are currently really in a position to make independent assessments.

Q385 ***Lord Lyell of Markyate:*** The Civil Service whitewashes it, does it?
Professor Sasse: I could not possibly comment. Also, to be fair, this is a process that happens quite often in political life and it is understandable that different stakeholders try to exert influence. There is another case which was about how effective biometric recognition techniques were where in another country influence was clearly exerted to make the findings of a study look much, much better than they actually were, or where reports were being withheld.

Q386 ***Lord Rowlands***: When the police gave us evidence on CCTV, they accepted the point about crime prevention but they said there had not been any evaluation on crime detection and that if there had, there would be a better assessment. I do not think I bowdlerised their evidence. They also told us that they do do evaluations on DNA, they have to.
Professor Sasse: They do evaluations . . . ?

Q387 ***Lord Rowlands:*** On the value of DNA in terms of crime. I thought one of the witnesses said that. I will check it out.
Professor Sasse: Basically the evidence that has been presented is anecdotal and it presents cases where it helped to solve the crime but, as Martyn said, very often it is not necessarily very clearly investigated whether the conviction could have been assured by other means, whether other evidence would have led you to the same conclusion.

Q388 ***Lord Rowlands:*** In the most recent case the evidence was that CCTV and DNA in that case played a very particular role. You cannot say you would have found it anyway. Why not accept the value of that evidence?
Professor Sasse: Because you have nothing to compare it with.
Professor Thomas: That is a very dangerous argument. You could use it to justify torture.

Q389 ***Lord Peston:*** Many countries do.
Professor Thomas: Absolutely. So that argument is not a strong argument for using a technology. The fact that, on occasions, it has proved to work, does not give you any information at all about whether it is a cost-effective way to use your resources and you have to put in the balance the potential risks to the population at large of holding that sort of data about people.

Q390 ***Lord Rowlands:*** I do not accept your argument making a comparison between torture and actually just collecting CCTV evidence of the kind we are talking about.
Professor Thomas: I am merely demonstrating the nature of the argument: I am not trying to equate the two issues.
Lord Rowlands: But you did.

Q391 ***Lord Morris of Aberavon:*** There is nothing new in this; we have had fingerprint evidence over centuries.
Professor Thomas: And interestingly, when there was a serious evaluation of the value of fingerprint evidence, it turned out to be scientifically pretty shaky too.

Q392 ***Baroness O'Cathain:*** May I just track back a few sentences to what you said about evaluation of the value of CCTV cameras and you said that the police more or less said that they were not that valuable? Can you put any sum of money onto the deterrent effect? The ordinary man or woman in the street actually sees something and knows they are on camera and I am sure there is a deterrent effect in that and that does not seem to come into your equation.
Professor Sasse: Criminologists do factor that into account and there was a report on that.

Q393 ***Baroness O'Cathain:*** How do they know what I am thinking and then I just suddenly think I am being looked at so I will not go and nick that cutting in Wisley or wherever?
Professor Sasse: What for instance I can tell you is that maybe CCTV causes crime to drop in the area where you have deployed it, but then it increases in areas that are bordering it, meaning effectively you are just displacing it.

Q394 ***Baroness O'Cathain:*** Is it not universal now?
Professor Sasse: No.
Professor Thomas: It turns out that CCTV cameras make people fear crime less but the crime that they principally fear is violent crime and most violent crime is not premeditated. If you were to take evidence from the Probation Service, they would tell you one of the biggest reasons why violent crime exists is that people cannot control their emotions, either because of the substances they have been taking before the crime or simply because it is in their nature to find it difficult to control themselves. Under those circumstances the presence of CCTV has no deterrent effect whatsoever. The studies show that the deterrent effect of CCTV on violent crime is actually very small and whereas there is a strong displacement effect of other sorts of crime, for example breaking into vehicles, you can actually reproduce an equally strong effect simply by improving street lighting. Better street lighting, particularly in areas that are very poorly lit, also has a very powerful deterrent effect on premeditated violent crime like people lying in wait for women and sexually assaulting them. So it is worth carrying out proper, ideally academic—Lord Peston and his colleague should be the people doing the evaluation work—proper evaluation of the different strategies that are going to be deployed and then making your policy based on sound evidence, rather than on how people feel.
Dr Forbes: May I add something from the social science perspective? One of the reasons that the results of the studies into CCTV seem counterintuitive is that we begin with the assumption that this single thing, CCTV, is the crucial thing which we will then test. However, there is not ever one crucial thing in terms of human behaviour; it only ever makes sense to consider a range of things. All these studies show that CCTV may work to reduce crime levels in an area in association with a whole series of other measures, also street lights to make the CCTV terminals work. So what these studies always show is that there is no single thing that you can do to change a human's behaviour—apart from kill them—and that is the way that the social science evidence will always lead us, to say let us think of this in a more complex way, let us see this in a nuanced way. We have to release the instinct to say there is an answer and we can find it and we can implement it and thank goodness it is technological, because it is going to be cheap and it is going to be easy to do. I am afraid that all the studies will show that is never going to be a possibility; that is just not the way humans are.

Q395 ***Lord Peston:*** Of course I agree that we must study these things properly, but we do run into the problem, following Lord Lyell of Markyate's question to you, that people are irrational. So, for example, whenever I ask anybody about CCTV cameras, they tell me they make them feel safer. Now, if we go back to my favourite area, we know in the area of risk taking that our aircraft are ridiculously safe. If we look at how people manage their own affairs in their own households, they take enormous risks, but if you were to say—and as an economist I have always argued—that the risk taking in their household is how safe our aeroplanes ought to be then they say "No way", if people feel that CCTV cameras are a good thing and they feel safer, then do we not have a problem when saying all our research shows you are wrong because they say "Well, we still want the CCTV cameras"? Look at local authorities who are putting them up all over the place for no obvious useful reason, except that they think their electorate wants them. What do we do?
Professor Thomas: If the reason for doing it is to make people feel safer, then you do not need to record the images and you do not need to retain them.

Q396 ***Lord Peston:*** I do not disagree with that, but a lot of the evidence is that we do not need these cameras under any circumstances, except that people want them.
Professor Thomas: Absolutely, in which case, if the reason that you are putting them there is because people want them, you do not need even to connect them up.
Lord Peston: I agree and of course your point, which it had not occurred to me until you made it, about better street lighting, is an enormously powerful point and it shows that evidence can affect people; it affected me just now anyway.

Q397 ***Lord Lyell of Markyate:*** You were saying that it merely displaces crime, but that is very valuable. If it displaces it, quite obviously the potential criminal is going elsewhere; that is what displacement means. So it is influencing crime; that must be true. If you were to be able to get the police to turn up quickly, which is much more difficult, it would have an even more deterrent effect. Is that not correct?
Dr Forbes: It is true that there is some evidence that it displaces, but that then tells you that CCTV is not reducing crime, it is only moving it.

Q398 ***Lord Lyell of Markyate:*** Well that matters to me.
Dr Forbes: It depends where you are; not if you are where they go. If it is displaced towards you, you would not be happy about it.

Q399 ***Lord Lyell of Markyate:*** I am a shopkeeper.
Dr Forbes: There are communities where that is the case and it tends not to be the better-off communities where that crime is displaced towards. That has to be a concern in terms of social justice. We are not going

to spend taxpayers' money to make sure crime only happens to the poor. That would be an interesting decision to see discussed in public. So, it is not going to reduce crime, it is going to displace it; that is an issue. You were also concerned about . . . ?

Q400 ***Lord Lyell of Markyate:*** I was picking up your argument and it seems to me you are getting over-theoretical and that there are actually practical effects. Okay, if there are more in a middle class rich area than there are in poor areas, that is an argument for having more in poor areas too. It is not an argument for not having it at all.
Dr Forbes: That is the fallacy of composition (to be theoretical). If I take a box to a football game because it will help me see over the people and then if everybody takes a box, I still will not be able to see over everybody. So merely displacing it, if you are not reducing it, is going to keep it moving around and keep happening.

Q401 ***Lord Morris of Aberavon:*** May I tell you, as a former constituency member for many years, that the public are very pleased to have CCTV? I am pleased to have CCTV in the development where I live in London and we do not distinguish between violence, however you describe it, and car crime. May I ask you whether there has been a cost benefit analysis of street lighting and CCTV as regards to their effectiveness?
Dr Forbes: Not a direct one.

Q402 ***Lord Morris of Aberavon:*** Is that not important?
Dr Forbes: The cost of street lighting is cheap compared with CCTV.

Q403 ***Baroness O'Cathain:*** What about emissions and light pollution?
Dr Forbes: CCTV uses light, it uses power, it uses people, it uses resources. By comparison, street lighting is relatively cheap. I agree that people want and like CCTV and if they want it and they like it, there is no reason why they should not have it. However, there is no reason for us to say to them that it will do things it will not; they think it will do, but it will not actually do. We cannot also give it to them and lie to them about it. We should say if they want it, they pay for it.

Q404 ***Lord Woolf:*** Anybody would agree that in this country we are good at carrying out research as to the sort of things we are talking about and I am sure the benefits of the research would be very considerable and enable us to use our resources better. May I just come back to DNA? The situation with DNA is very different from what we have just been talking about with CCTV cameras. You look sceptical, but why I say that is that there are crimes which are almost impossible to prove without DNA where the man says "I never had sexual relations with the woman" and the woman, because of the nature of the crime, is in a situation where there is no external corroboration of what she says in many situations and therefore DNA can play a critical part. I am not saying that there is not still an evaluation to be done but that is a huge benefit. Would you agree that we must not lose the baby because of some of the things that you have been talking about and what really is needed is greater care as to how we use data and how we protect it when it is not being used?
Dr Forbes: I agree with that.
Professor Sasse: The DNA database is certainly also an example, if we are talking about the legal framework for it, where there is a great amount of insecurity. I was at a meeting two weeks ago where one of the chief constables associated with running that DNA database said that a High Court judge had issued an order for DNA out of the DNA database to be released to be used in a paternity case. If a High Court judge can make that mistake, that the legal foundation of the DNA database is solely for the detection and prevention of crime, the law just is not very clear. May I say that police officers, for instance, are all fingerprinted and their fingerprints go into the National Fingerprint Database for the purpose of exclusions. The Police Officers' Federation has consistently refused to do the same for DNA exactly because they are worried about potential mission creep, potential further developments of the technology and they say, for instance, they are worried about it being used in paternity cases.

Q405 ***Baroness O'Cathain:*** That is a crime too.
Professor Sasse: What, paternity?

Q406 ***Baroness O'Cathain:*** Yes, it certainly is.
Professor Sasse: Today a case is being heard in the European Court of Human Rights. Originally the legal basis for the DNA database was that only people who were convicted of an imprisonable offence would have their DNA retained in the database. That was subsequently changed and now we have this discussion about the fact that once you have dropped litter your DNA is going in the database and people have had to go to court and go to quite serious lengths to have their DNA removed from the database because they were questioned but never even charged and they certainly were not convicted of anything, yet their DNA remains in the database. The fact is that that information is not just unlocked when you have a match, that is that there has been a crime and there was DNA at the crime scene and now there is a match to something in the DNA database that basically unlocks your record, you can also search and the name is against the individual. It has all sorts of implications that are

often not thought about, such as the number of people whose DNA is in the database is completely disproportionate at the moment. You will remember for instance that something like 50 per cent of black males between the ages of, you know. One High Court judge said that we should either put everybody's DNA into it or rethink how we collect it, because it is clearly unfair at the moment.

Q407 ***Viscount Bledisloe:*** May I take you to another passage in the research paper, paragraph 21, where you say " . . . few public-sector developments . . . plan or budget for adequate security of personal data". Two questions. First of all, could that be overcome by better public procurement specification but, secondly, is it the planning of the system that is the real problem or, as was rather suggested to us last week, is the real problem careless or occasionally ill-intentioned people who have access to the system and either leave the data lying around or actually extract it to give to their associates not in the business who want to see it?
Professor Thomas: The short answer is: all of the above. There is a fundamental weakness at the heart of the transformational government agenda which is that you cannot build large databases that are accessible to a wide number of people and maintain a high degree of security. That is something that the military acknowledge; they would never allow a secret database to be accessible to a wide number of people, for example. For technical reasons it is very difficult to build a database that is technically secure on top of commercially available, off-the-shelf software components, because almost all of them were not designed to support such a use, and to connect such a database to the internet simply creates a honey pot that virtually guarantees that the data will be extracted from it in a way that was not planned for or intended. Something that I would hope you could influence is that there is guidance in the Manual of Protective Security on how to carry out impact assessments on what the likely impact is of loss of personal data and on how such data should be protected. That manual is classified. As a consequence, it has not been peer-reviewed because it is only available to people whom government departments believe have a need to inspect it and that is largely restricted to companies who are engaged commercially in building such databases for the Government and who therefore have a vested interest simply in going along with it. If you could enable at least the personal data part of that to be made publicly available so that could be thoroughly peer-reviewed, I would expect that that peer review would lead to significant strengthening of the protection that was required of personal data because it would be seen to be clearly inadequate.

Q408 ***Viscount Bledisloe:*** Assuming that were achieved, would that then accurately succeed in protecting the data or would one still be at the mercy of the negligent or ill-intentioned individuals?
Professor Thomas: You will always be at the mercy of the negligent and the ill-intentioned. If data has a value to somebody and it is accessible to a wide number of people, there will always be somebody who can be corrupted to make illegal access to that data.
Professor Sasse: The Information Commissioner's Office recommends that a privacy impact assessment is carried out prior to the design and implementation of any system where personal data would be held. I believe that if that were done competently and honestly, it would lead to much better protection and it would lead to less off-the-cuff decisions about what data to collect and how long to keep them for. If it is done competently and honestly, it also has a big pedagogical effect on the people in a company, so they learn how to do things better, they learn what to care about. Finally, would people really care? That partly depends on the legal safeguards that you have. The fact is at the moment that the fines the Information Commissioner's Office can hand out when they find that people are breaking the law are very small compared to the profits that are being made by trading illegal data. In some European countries in about 2002 they changed the law to make it a criminal offence, first of all, if personal data were not being looked after properly or if they were collected in contravention of their data protection act. Secondly, what happened was that the responsibility was assigned at board level, so effectively what a country like Germany has is the equivalent of corporate manslaughter legislation for irresponsible illegal use of personal data. It certainly had a huge effect in that country. In those countries, what you now get is people at the top of the organisation really taking an interest and making sure that the company is run and processes are set up in a way that takes proper account of these things because they do not fancy going to jail.

Q409 ***Viscount Bledisloe:*** I want to go back to the point you were making earlier, that if the penalties for it being misused are high enough and hit the people at the top, then more elaborate specifications would be made and fewer people would have access to it.
Professor Thomas: Yes, and some systems will not be built because it will be seen that the risk to the public is greater than the benefit that they would bring.

Q410 ***Lord Lyell of Markyate:*** This is very interesting. Could you just give a practical example of how the companies make money and ignore the small penalties?

Professor Sasse: Selling information that they have collected without consent on to other companies. The biggest penalty is passing it outside the EU, for instance transferring data outside the EU which is specifically prohibited unless there is a very good reason and case for it.

Q411 ***Lord Lyell of Markyate:*** What is the penalty?
Professor Sasse: They are relatively small fines.

Q412 ***Viscount Bledisloe:*** Limited by Parliament?
Professor Sasse: Limited by the DPA, the Data Protection Act, and by the powers the ICO has. It is just purely financial.

Q413 ***Lord Peston:*** The distinction that needs to be made is between the public and private sectors and in the private sector things are commercial in confidence which they enforce very strongly, but then of course, if their commercial secrets get out, that costs them real money so they build up a climate of what has to be confidential. Your argument seems to be that in the public sector, there are not the same incentives to create the culture of privacy because those who suffer if some data gets out are not the people in the organisation, it is people who are suffering. So the question we have to ask is how to set up a culture of taking privacy seriously. Lord Woolf totally demolished your view that you impose enormous penalties on the people because you could never enforce those penalties in practice could you? Therefore the point is how do you? Do you have views on how we develop this culture—I use the word on purpose—within the public sector of taking privacy very seriously indeed? There is the other side of course that in some sense you can overdo it. I had to ring the Inland Revenue this morning and we did not go through any of the usual nonsense of asking for my code number. I said "It's me", they said "What's on your mind?". I said "I think the tax calculations are wrong" and he just pressed a button "Oh yes, it has all come up here" and we are in business. If he were to take me through a whole list, as Barclays Bank will, of my favourite word and my number and this, that and the other, I would get so angry with them and so on. There is a two-sided thing that the individual actually benefits from not overdoing the privacy thing and I am just wondering whether you have worked through how you get the balance of creating the culture of privacy in the public sector right, with the desire of the customer wanting—in my case tax affairs, but it could be almost anything—dealt with very quickly indeed. Have you done work in this area on how you balance the two? You are not going to fire the head of the Inland Revenue. As far as I know, the head of the Inland Revenue was not even ticked off for losing those disks.

Professor Sasse: You do a risk assessment and you put in protection that is adequate for managing the risks that you care about. You can do that in a very economically guided way by doing an economic assessment of it and putting in certain protections, but also including values that individuals place on that privacy. Very often, where people say they do not actually care about it, it is because people are not very good at assessing risks in the future, because they have not experienced the impact or nobody they know well whom they would understand and empathise with has experienced these bad effects. When they do happen, and I have done research in this area, people get very angry when they were not aware what of themselves or their family was at risk because data was disclosed. If you have a chance to accept the risk and you say you would rather not go through all these questions and if any private investigator or anybody is trying to target you, any identity thief rings up the Inland Revenue and gets this valuable information, then you will live with it.

Q414 ***Lord Peston:*** I am merely saying there is a problem of balance.
Professor Sasse: You have to accept it.
Dr Forbes: Yes, the balance is something that has to be struck over and over again between the individual citizen and the agency and it seems to me that the way to go is to set up a charter of understanding such that every individual has to learn that they are making quite key choices here. If they give up certain information in certain ways, then that is going to have an impact on their privacy and their security because the Government cannot promise the earth in these situations. There needs to be much more of a realistic debate and discussion between Government and the citizenry about what it will put up with and what it will give and what it can expect and the Government need also to say that they cannot offer complete security on these things, that they can offer functionality up to a point and they have a range of options for you to look at and to develop and things will go wrong and if they go wrong, these are the things that will happen. It seems to me we have to move to a much more adult way of dealing with this. What strikes me when I look at this is that there is always a tremendous amount of media attention on government agencies losing data. I have never really seen any evidence of harm caused by that whereas I bet everybody around here has had credit card fraud perpetrated on them as an individual at some point. That is not Government. That is where the problems lie. That is not what gets into the media. There is a kind of disproportionate view about what risks people are prepared to take on a daily basis in terms of their money and the general outrage if there is some sort of citizenship information being bandied about or just lost; it is not really being stolen as far as

I can see. I would like to see a much more open debate about what Government are offering and they have to be much more accurate in what they claim a system can do because some systems are just impossible to create.

Q415 ***Baroness O'Cathain:*** On the basis that issues like this set up completely opposite reactions, my reaction to the comment that Lord Peston made is completely different. I would be furious if I rang up the Inland Revenue and they knew all about me without going through checks. When I get onto my bank, I am delighted that I am asked what my favourite colour is. That is fine. I am wondering, back at the ranch, about the training of information professionals. Are they really aware of the need for privacy and, for example, going back to the HMRC and the DVLA data that were stolen, why were they not encrypted and is there some reason that it is too difficult or is too much power in one or two hands who could do the translation into normal data? If we can start off with a good training programme for people who are involved in the industry, that is where it has to start. I just wondered what your views were on that?
Professor Sasse: My view would be that I would be concerned that in the training of information professionals, if the training worked properly, they should not design a system that allowed any junior person to walk up, stick in a CD and take a whole copy of records without any alarm bells going off anywhere. Martyn knows a bit more about this. Training of security professionals is something that has been developing more rapidly in the past few years, but ultimately it is also down to the customer. It is the people who are commissioning and paying for the system who should have to be clear about what their security requirements are. Ultimately, the company who is building the thing will only give the customer what they ask for. They may raise a few points but currently we really have a problem that the customers often do not articulate their security requirements, they do not think about them.

Q416 ***Baroness O'Cathain:*** Because they do not know. Those people who are commissioning something like the National Health database would not really know. Why would they, because that is not their job? It is a very difficult thing and I wonder how you bridge that.
Professor Thomas: It is a complex issue but it is an issue like safety. Safety is equally complex and it requires proper hazard analysis to be carried out by people who are skilled in carrying out hazard analyses and then an appropriate set of protections to be put in place to address each of the hazards. That is what taking privacy seriously involves. It means using the appropriate technical means and the appropriate social means to ensure that, firstly, you have understood the level of privacy that you are seeking, what level of breaches of confidentiality do you regard as tolerable for example, and then, having set some targets, that you actually build the business processes, the social systems, the training and the technology to deliver that level of confidentiality in the systems that you are building. At the moment, that analysis appears not to be being done. There is no technical barrier to it being done, but it would lead to a lot of systems turning out to be a lot more expensive or not practical.

Q417 ***Baroness O'Cathain:*** That is actually counter to the way society as a whole is going. We are told all the time to be transparent, we have investigative journalism, we have all these issues where people gossip, knowledge is power and all this mass of information going around on the net. None of it is like those posters that you see in the Imperial War Museum "Keep quiet and don't talk", or whatever it was. I just feel the genie is out of the bottle and I am wondering how the genie is going to be put back into the bottle.
Professor Thomas: We have done some work with the Y Touring Theatre Company which is the YMCA's touring theatre company which is trying to introduce the messages from the Royal Academy of Engineering report to schoolchildren. That has been really very revealing because, for example, we met with a group of schoolchildren and explained to them that if they put photographs on their Facebook page and then a few days later took them down, they did not go away, and they were shocked. We have a generation of people, not just the young people but their parents as well, who simply do not understand the risk that they are running because there is not a full understanding of how the internet works and therefore, information is revealed which feels as though it is local to Tesco or, yes, it is on my web page but I can always take it down. No you cannot; Google has got it, it is in the cache, it will be there forever.

Q418 ***Lord Peston:*** Two years on Google.
Professor Thomas: Perhaps.
Dr Forbes: That is what we can do: require people to have policies that say stuff expires, that technologically it is going to expire. We could insist on that, certainly in this country, and then get it through Europe and the world is a problem of course but that is one of the things you can do. If I may give another aspect of the genie being out of the bottle, there are lots of elements in the public sector which do have a culture of privacy which have been brought up with understanding the importance of an individual's collection of information in the Health Service, some parts of the criminal justice system and

schools. A lot of basic training has already happened. The problem is that they are not fully able to understand the technology and too many times it is just too easy to shift some data without ever thinking about the privacy implications of it. That is where the training goes. We do not have a deep problem with no culture of privacy in our key organisations. The problem is that the way the technology is intervening has made it just something that does not happen at a very low level, a seemingly trivial level too often.
Chairman: The wartime slogan you were thinking of was "Careless talk costs lives".

Q419 ***Lord Norton of Louth:*** Looking at a slightly different aspect, the relationship between commercial data and data that are kept by the state, UKCRC's evidence stresses the extent to which personal data are collected, stored, exchanged among commercial companies but in paragraph 13, you say "Once collected, commercial data is available for use by the state". That statement is not qualified. Can you give examples of where that happens and, conversely, how much data collected by the state is then made available to commercial companies? I can think of one or two examples where that happens, but how extensive is it and what protection is there, what safeguards are there that cover the exchange and are they adequate?
Professor Sasse: A variety of commercial data is used by Government, particularly for criminal investigations: phone records, mobile phone call records, location records and credit reference agencies. In the biographical interviews being conducted for the national identity register they are making quite extensive use of data that credit reference agencies are holding. There have been examples; one of the members of our body reported that his hospital trust sold patient data on to a third commercial party through a combination of ignorance and the temptation to use it for a particular purpose which was just too high.
Professor Thomas: PCTs have been required to give health data to the Immigration Service, for example, in an attempt to track down people who have overstayed their visas, leading to people who had overstayed their visas and who were, for example, infectious with tuberculosis disappearing because they could no longer risk going to get medical treatment. You do get unexpected side effects from these things.

Q420 ***Lord Norton of Louth:*** How does one safeguard against that? I remember discussions we had on things like making the electoral register available for commercial purposes. Are there safeguards just generally on the transfer of data in that form? Are they adequate?
Professor Thomas: Given a particular requirement, you can usually build a safeguard that is adequate for the purpose, so it will not be a one-size-fits-all.

Q421 ***Lord Rowlands:*** May I return very briefly to the earlier evidence when I referred to the police evidence given to us. I now have the text in front of me. It was in answer to question 147 and it was Deputy Chief Constable Gerrard who said "We were required through Her Majesty's Inspector of Constabulary . . . to justify the expenditure around DNA . . . we are required to record the amount of crimes that are detected, both primary detection and secondary detection, offences taken into consideration, that come from both fingerprint and DNA". He contrasted the fact that there was an evaluation process with DNA but there was not one with CCTV but they could do it. There is a cultural perspective and we have received evidence. Do you think this is either marginal or what?
Professor Sasse: What that does is compare the expense on DNA and fingerprinting and how it is being used for convictions and that comparison makes the DNA database look quite good.

Q422 ***Lord Rowlands:*** It is not a bad basis for evaluations, if it is helping to detect crimes.
Professor Thomas: It is an uncontrolled experiment. It does not tell you what would have happened were the resources, for example, spent on more policemen.

Q423 ***Lord Rowlands:*** There is an evaluation of some kind taking place on DNA. Can I refer to your evidence where you say "All surveillance changes the balance of power between the watcher and the watched, so the increasing collection and sharing of data by public-sector agencies self-evidently has constitutional implications"? As a Constitution Committee we are particularly interested in that. What specifically are these implications and how can we address the constitutional implications?
Professor Sasse: To me a key one is the relationship between Government and the citizen, which is changing because the presumed-innocent-unless-proven-guilty stance that we have is being eroded in favour of going, if you are familiar with that movie, towards what we call the department of pre-crime, that information is justified, that information is collected and used quite extensively because it could be used to prevent crime. This went all the way to Tony Blair who, towards the end of his period, was proposing that you could assess the risk of a foetus in the womb turning into a criminal by profiling the family and background. I just find that incredibly shocking because, if you look at this as a social scientist, if you fall into certain profiles or certain groups, the suspicion is cast on you. It makes it all that bit harder for you, if you are being marked out

like that, to turn out against the circumstances and turn good and this kind of profiling and aspersion erodes the normal relationship. Effectively the Government say to citizens that they are not trusting them, they are going to collect any information on them that they can and are going to hold onto it. To quote some policemen friends of mine, they will always say "What shall we collect? How long shall we keep it?" and they would say "Everything and keep it forever because you never know when it might come in handy". Whilst I can understand them making that argument, it completely erodes the basis of trust between the citizen and the state. People who are not trusted tend to react against; the people who are not trusted behave worse than people who are trusted.

Q424 ***Lord Rowlands:*** What sort of constitutional safeguards should we be building in? We are now discussing constitutional implications, so can you give us any thoughts about what constitutional safeguards we should be building into the system?
Professor Thomas: It seems to me fundamental to democracy that, firstly, everybody starts equal and, secondly, that the citizens can hold their Government to account because it is after all their Government. It is not that we are the Government's citizens: it is that the citizens come first and the Government is elected by those citizens. The more information that is held and processed in a way that is mysterious to the citizen, the harder it is to hold the Government to account for its actions. So it seems to me that transparency and reciprocity in visibility of what is going on become absolutely fundamental to democracy.

Q425 ***Lord Peston:*** I do not know whether legally everybody has to have a name. I think everybody has to have their birth registered but could a parent say their child is not going to be given a name as far as you know? The reason I ask the question is that I have never understood, other than it would take 100 years, what the difference is between a person's name and their DNA, because both simply say this is who I am. I agree we might object to the DNA database because it would take 100 years from birth today right through plus the costs; there are arguments. In so far as I understand it, DNA is the equivalent of who I am, namely my name.
Professor Thomas: It tells much more about you. It says who your parents are, for example.

Q426 ***Lord Peston:*** It does on the birth certificate also.
Professor Thomas: The birth certificate says who it was alleged your parents were.

Q427 ***Lord Peston:*** Is it not helpful in a democracy to be able to identify every person? I was shocked by your piece of evidence a little while ago that the police, not even the police attending the scene of a crime, have to submit their DNA. Is that right? I find that staggering, I am with you on that, but I still do not see the argument why one would not record everybody's DNA at birth.
Professor Sasse: As Martyn says, your DNA gives away a lot about you and it means then, if, for instance, you carry a certain genetic defect, you are immediately screened out and treated differently.

Q428 ***Lord Peston:*** That is the use point, which is your other argument. I am simply asking what the argument is other than cost or we cannot wait 100 years?
Professor Thomas: So long as it is universal there is actually no argument because, after all, your DNA is not private. If I take your cup away when we leave this meeting, I have got your DNA.

Q429 ***Lord Peston:*** That is why I was so shocked by what you were saying about the police.
Professor Thomas: But if I did collect your DNA and process it and analyse it and start looking at your familial relationships, you would have every right to feel under some kind of threat and a bit affronted.
Lord Peston: I am not the sort of person who feels threatened but others might do.

Q430 ***Lord Rowlands:*** May I get back to the point about the specific constitutional safeguard that we might be looking at? Are there any constitutional safeguards in any states outside ours which would be a good example to follow?
Dr Forbes: I am not aware of any.
Professor Sasse: It might be worth looking at the German model.

Q431 ***Lord Morris of Aberavon:*** May I ask you about the RAE report on dilemmas as regards technology? The burden of the report seems to me that the law has not kept up or, if it has not, the alternative that it should keep up with the development of technology, that the law on privacy should be clarified. What exactly do you mean by that? Does it mean amendments to the law or more powers to the Commissioner?
Dr Forbes: Certainly the Commissioner should have more powers. It means new legal arrangements, new legal provisions arising out of these changes. There is a discussion about the person and the DNA. The whole issue of identity and digital identity takes us into a grey area where it is not specified very clearly in the law where the rights begin and end, particularly

between the citizen and the state because there is a lot more collection of data which allows the identification of an individual. Previously that has not been the case and you have not been able to work backwards very easily to a private individual but the increasing amount of data that is collected makes that more possible and it is a software operation, so it is a technological operation. There are cases for the law stepping in and making clear where the boundaries, at the moment, need to be set and what the consequences of stepping over those boundaries are. There has been quite a lot of change in our understanding of territoriality, in terms of our legal sovereignty, because of the internet. There is the whole issue of child abuse and storage on what used to be regarded as sacrosanct and personal items like computers and which now can be subject to legal process in the home. That is the kind of change. Because the technology has come into the home in a particular way, so the law has had to come into the home in a particular way. Those are the sorts of examples I would be thinking about. How long will it be legal for somebody to send me Spam? Nobody wants it, I cannot stop it, I cannot find out who is responsible and these are the areas where the law needs to be stepping forward.

Q432 ***Viscount Bledisloe:*** You are suggesting that there are differences of views about what counts as reasonable protection of privacy. May I give one example from your own papers? The Academy of Engineering say in their report that the retention and sharing of data about individual's health is essential and that that must be done, whereas the Computing Research Committee says that there is certain data which people legitimately need to keep private, for example HIV status, mental illness and traumas such as rape. I suspect that on reflection everyone would agree with the second view and that the engineers have rather overstated their position. First of all, do you agree about that? Secondly, how does one deal with it? Do you have certain categories of medical information, such as those specified, which are not to be shared unless I consent and otherwise, on top of that, a general right for me to say I do not want this, that or the other or maybe any of my medical history passed around?
Dr Forbes: There is no conflict here. If any individual gives information to a health professional and they store it and they record it, there is no problem in terms of privacy of that being shared with the next relevant health professional, like when the doctor changes, leaves the practice, you are still there, you want that record still there and you want that given to the new doctor. Even without my consent I want the relevant medical information used where it might need to be used, if I am unconscious or something.

Q433 ***Viscount Bledisloe:*** Suppose I think I may have HIV and I deliberately go to a doctor who is not my normal GP because I do not want to tell my normal GP what I have been up to. Surely I will not want that passed back to my doctor without my consent.
Dr Forbes: It seems odd, because if you have got HIV, that is information that the medical services personnel does have to have in order to treat you effectively; that is the contract. They have to know who you are, what your situation is, before they can be expected to give you any medical treatment.

Q434 ***Viscount Bledisloe:*** I may prefer to be wrongly treated rather than have this information disclosed.
Professor Thomas: Yes. I was involved in writing both these statements which you say are conflicting. The Royal Academy's point was that population-wide data is extremely valuable to the country, but that it ought to be anonymised, that the individual ought to have control over the link between their private data and their identity, particularly for the most sensitive personal data and what is sensitive will differ very much depending on the individual. If, for example, the summary care record is made available on the internet so that people can check their own health records and that summary care record contains prescription data, which is what is currently intended as I understand it, then that will put at risk, for example, a Muslim young woman who is taking contraceptives without the knowledge of her family and who can be placed in front of a computer in the security of her own home and forced to log in and reveal that medical data. So you get risks that differ by individual or type of individual and it is essential to set things up so that the defaults are safe right across the population and that people then have the right to open up the freedom of access. To set up a set of systems that put a sub-category of the citizenship at potentially serious physical risk seems to me to be unacceptable.

Q435 ***Viscount Bledisloe:*** I have no problem with the theory that the world should be entitled to know how many HIV people there are in this country, how many people there are taking the pill, but surely I must have the right to prevent even my own doctor knowing that, if I do not want him to.
Professor Thomas: I would agree with that.
Dr Forbes: Nobody would know whether he did or did not.

Q436 ***Lord Morris of Aberavon:*** We have gone through dozens of different scenarios. Should they not be looked at and have to be looked at case by case? The law after all is only a mechanism to put into effect ideas and who should reach a judgment on each of these cases as to what is proper and proportionate and appropriate?

Dr Forbes: There is definitely a case for "horses for courses" because without a doubt there are different things which require different arrangements. It is also true, all the studies show, that there are certain specific problems with the security of data, that we need to have a higher standard of design and a higher standard of practice across the board and then, in those individual cases, you very specifically design something that is going to serve your purposes.
Professor Thomas: The Health and Safety at Work Act has a blanket requirement that risks to safety of citizens should be reduced as low as reasonably practicable. That phrase "reasonably practicable" was defined in the Appeal Court very specifically to mean that the cost of reducing the risk further would be grossly disproportionate to the benefit that would come from doing that. I can, if you want it, provide you with a reference to that judgement, but it is on the HSE website as well. It seems to me it would be ideal to have exactly the same form of words in law when it comes to protecting privacy, that the risks of breach of confidentiality should be reduced as low as reasonably practicable.

Q437 ***Lord Peston:*** I was very intrigued by the RAE's recommendation about organisations needing to authenticate individuals' entitlements. You say that they should use the minimum information necessary rather than requiring people to identify themselves, whereas I would have logically argued that requiring people to identify themselves is the minimum information necessary. Is the minimum information the fact that we have all got a national insurance number? Would that be what you had in mind? What is the minimum?
Professor Thomas: No.
Dr Forbes: Just take the example that Martyn used earlier. To use the Underground I could buy an Oyster card. You do not need to know who I am to go through that. I can be authenticated by using the Oyster card; I have permission to go through. There are lots of cases where all you need to know is that I do actually have permission, that there is some arrangement that has been made that gives access to this person with this bit of information that can be transmitted and recognised. Most of the time, it seems to me, I am asked not for a simple piece of data which gives me access but I am asked for my postcode. Suddenly they know who I am, where I live and they do not need to know that and lots of times I do not want them to know that because I suspect that I am getting junk mail because of some of these questions being asked. Even though you look very carefully to see how to stop that happening, still lots get through. I use different forms of my name so I know that junk mail that comes through is connected to that illegitimate use of my data. If I were just authenticated, they would not know who I was; they would not be taking my data and using it for their purposes. There are lots and lots of cases where that is all you need to be authenticated. If, for example, you are buying something over the internet, who knows who is at the keyboard? They do not authenticate the person.

Q438 ***Lord Peston:*** I have misunderstood your evidence. I thought you were talking about things like "I am a single mother entitled to child benefit" or "I am disabled and I am entitled to these benefits".
Dr Forbes: Absolutely; yes.

Q439 ***Lord Peston:*** But one of the disgraceful things is that if I am disabled, the form I have to fill out requires the brain of an Einstein, let alone get the benefit. Certainly I have tried filling out such forms for other people, but I thought that was what you were talking about.
Dr Forbes: No, it is about over gathering data.

Q440 ***Lord Peston:*** I understand your point about over gathering, but where you said "individuals' entitlements", I thought you were talking about public services and what I am entitled to because of my specific condition; about my specific condition; whether I am disabled or a single parent or this, that or the other means knowing very precisely who I am.
Professor Thomas: No, it does not actually. It means knowing what your specific condition is.

Q441 ***Lord Peston:*** Therefore *a fortiori* I would have thought your argument would be the reverse: you need to know that detail but then you need absolutely to protect it from anybody else getting near to it.
Professor Thomas: Actually very rarely do you need to know who somebody is. If you have to have a proof of age card that shows you are entitled to buy age-protected goods, why does that need to have your name on it? There is no reason why you should communicate to somebody selling cigarettes or alcohol or letting you into a film what your name is because that is completely unnecessary.

Q442 ***Lord Peston:*** What about my travel pass? You definitely need a proof of age to get your travel pass.
Professor Thomas: You need a proof of age to get the travel pass. Once that has been established, it does not need to say who you are.

Q443 ***Lord Peston:*** So everybody could use the card.
Professor Thomas: No, you can have a photograph on it. It needs something to link it to you but it does not need to be your name.

Q444 ***Lord Peston:*** With my photo almost anyone could get by.

Professor Thomas: Having your name on it is not going to stop somebody else using it because your name is not tattooed on your forehead.

Q445 ***Lord Peston:*** What I am really trying to say is that we are making a bit of a song and dance about this, when the real issue lies elsewhere. To go back to your example, you said you do not want anybody to know about your Oyster card, so you pay cash. Now that is up to you, but it does seem to me to be slightly ridiculous, if I may say so, though it is your choice.
Professor Thomas: No, no.

Q446 ***Lord Peston:*** You are entitled to make that choice and I am not trying to stop you. I thought we were talking about people entitled to things from the public sector where it is vital we get the right person.
Professor Thomas: There is a fundamental point here. Most people, for most of their lives, do not need to conceal much about themselves but some people, and probably most people at some time in their lives, need to conceal something. If everybody in general gives information away, it makes it very hard for the people who have an entirely legitimate reason—they are trying to escape an abusive relationship and they do not want the details of where they are currently living to be known—and you need to give those people the freedom to behave in a way that does not immediately highlight them as somebody with a problem.

Q447 ***Lord Smith of Clifton:*** The CRC says that the same technology is capable of affecting different individuals or different groups in very different ways and it underscores the Royal Academy of Engineering's concerns over the inequality by pointing out " . . . there will be some individuals and groups who benefit and some who are harmed". Can you give some concrete examples of these differential effects? Do they raise human rights issues? How might these problems be addressed?
Dr Forbes: There is a range of examples but not very many. One is the way that some call centres know who you are when you call and they then check you against their database, whether you are a big spending customer or not. If you are, you will get through immediately whereas everybody else gets shoved down the line and they are waiting for 15 minutes, except if you are waiting 15 minutes, you do not know that is what has happened, you do not know that is their policy and it is a clear discrimination against people on the basis of their spending power. That might be okay if you are informed, but you are not. Then, by inference, we know that discrimination occurs in very predictable ways across society within organisations. There is institutional discrimination and we are talking here about organisations which do not have to reveal what they are doing, why they are doing it, how they are doing it. They do not have to assure us that they are not being indirectly discriminatory, that is to say not meaning to discriminate against ethnic minorities or economically disadvantaged people, but that is in effect what they are doing without justification. We are talking about dealing with huge groups of people, so we could expect that some systematic disadvantage is going to be introduced just because people have not been trained to do otherwise. They are not trained to deal with data, they are not trained to deal with understanding that all organisations need to implement the social values to which we subscribe and for which there is specific law in relation to the provision of public services and private services. The predictable or usual suspects get disadvantaged here. For example, we have already had the evidence about the number of black people on the DNA database. What is that all about? That seems to me to exemplify discriminatory assumptions about a group in society; that they are more criminally active and more likely to commit crime.
Professor Thomas: And reinforces those views.
Dr Forbes: And reinforces those views. We know that it is in fact not the case. I guess we know since the big Sex and Race Discrimination Acts of 1975 and 1976 that unless you take active steps to reduce discriminatory behaviour it continues. In this area there are not, as far as I can see, active steps being taken by any of the organisations or required in any of the legislation to address these issues. Software programmes are being written which embed assumptions and stereotypes. The classic example of course goes way back to St George's Medical School which used to pride itself on the range and the ethnic diversity of its input until somebody looked at the programme used to select and it noticed that they offered places to the people with lower scores. If you were a woman, you got an extra 10 points. If you were from an ethnic minority you got an extra 20 points. So anybody filling out these forms was unintentionally, unknowingly, leading to a discriminatory output. Unless we know how these programmes are written and unless they are proofed in the appropriate way, then we can actually predict that they will discriminate. In my view direct action needs to be taken.

Q448 ***Lord Lyell of Markyate:*** Why do you say that was unintentional?
Dr Forbes: The person filling in the form gets the form, they fill in the age, the gender, the ethnic origin and behind that, the computer assigns value to it. It produces a printout, top of the list lots of white males and some white females and some very, very bright Asian candidates and they are the ones offered the places. The person doing the data entry had no idea

that the programme writer put those values on at some point in the past.

Q449 ***Lord Lyell of Markyate:*** Yes, but St George's meant it; they were intentional. That is exactly why they did it.
Dr Forbes: Yes, the person who wrote it intended to do that and it may have been legal when it was written. This was in 1980. It may have been legal before 1976 and 1975.

Q450 ***Lord Rodgers of Quarry Bank:*** Because the audiology technology of the House of Lords is sometimes defective I may have missed some of your replies so forgive me. Going back to the RAE report, it recommended a digital charter which would have a significant effect on the levels of trust. What effect do decreasing levels of trust have upon the democratic governability of the country? Would a digital charter add any real value to the policies, laws and other forms of protection which we already have?
Dr Forbes: On the question of trust, this is even more complex than CCTV because it cuts in so many different directions. I do not believe there is a general decline in public trust in Government but there are specific instances in which trust goes up and down. There are so many problems here. One is that there is misplaced trust in Government to do certain things that they cannot in fact carry out. Another is a misplaced distrust which is even tougher for a Government to handle because it is doing the best it can but it does not get credit for it. There is evidence that people do not believe that big data can be secured and yet we have governments continually introducing measures to deal with big data and promising that it will be secure. That is a real problem for Government. It needs instead to be more accurate and say "We can protect this up to a point. We can put these measures in which are going to reduce the functionality in some respects or reduce the risk in other respects and we need to talk about that". A digital charter, if it were to set out some clear bases for operation, some clear guidelines which the population and the Government could talk about and agree on where they are setting the balance, would be tremendously helpful for encouraging trust in this area because the Government rely on people to give accurate information. If you are the person who says actually you are not going to give information because you do not trust this, then that can do tremendous damage to the whole exercise of gathering the data. So it is quite important that we have trust in these systems and that we have trust in the exercise itself and the purposes for which it is being developed. We see a lot of examples of CCTV being used for public benefit but we see very little data which shows how data is effective in making good government, in allocating resources effectively or efficiently. A digital charter needs to look at all those issues so that in a consultative basis it allows people to say what it is that they want from these systems, from these digital systems; what it is that they expect. We know that in terms of trust people mostly think in terms of risk; how risky it is if they give you this information. So they will trust you if they think the risk is appropriate. They do not know what the risks are most of the time; they do not know what the expectation is. It is very difficult to know, so that is why I think a charter in advance is a way of getting people to come to a settlement for the time-being, to start a process which then can be reviewed in the future and evaluated to see exactly how well we are doing here. Otherwise it is just stumbling along, we do not have any guidelines and we do not have any sense of placing ourselves. It seems to me we need these things quite urgently because of the fast proliferation of technological mechanisms and means which take data out of our control and do things with it like data-mining and cross-referencing which we do not know is happening behind the scenes but which can have a huge impact on us as citizens.
Professor Sasse: May I add something to this which is an issue we have not raised so far and that is data quality? There is often an assumption when data is collected that it is all correct and it is all used in the right way. If you look at the reports by the Office for National Statistics, when you look at records you find that up to 40 per cent of records are either out of date or contain at least one significant false bit of information. To me that is something that should be enshrined in a digital charter, that citizens have the right to check the information Government hold about them and that it is corrected if it is not accurate. If decisions are being made about people that is one thing, but if they are made on inaccurate information that is another. We have had submissions from people who have said that their health records, for instance, incorrectly stated certain things and that they either had a very long battle to have that corrected—and that again is only something that the knowledgeable and the wealthy can afford to do—or even that they were told that there was no way that a record could be corrected if an entry was older than 90 days and therefore the best they could do was have post-its with "This patient is not an alcoholic" plastered all over the hospital to deal with the fact that the record was incorrect. That strikes me as an example of the duty of care needing to be that the records held are correct, that they can be inspected and they can be corrected.

Q451 ***Baroness O'Cathain:*** We have the right, have we not, to ask about our credit rating?
Professor Sasse: Yes, you have the right to see your credit record.

Q452 ***Baroness O'Cathain:*** So really what you are saying is that it is only Government that withholds the right to see the records they hold on us. Do we have the right to see records held by anybody else on us?
Professor Thomas: Yes, under the Data Protection Act.

Q453 ***Baroness O'Cathain:*** But the Data Protection Act does not extend to the government information being held on us.
Professor Thomas: It extends to a large part of Government. Unfortunately, you do not know who holds all the data so you do not know whom to ask.

Q454 ***Baroness O'Cathain:*** I am talking about NHS data.
Professor Thomas: Secondly, the Data Protection Act allows the organisation holding the data to charge you £10 for every database that has to be interrogated and that is just an impossible barrier to getting access to the data. You need a clear statement of who has data on you and then you should have free access to it.

Q455 ***Lord Peston:*** I do not want to appear an anarchist, but are we not right not to trust the Government? Is that not the nature of democracy? To take the example when Viscount Bledisloe asked you about medical records, if you were to ask the public at large "Who do you trust, the Government or your doctor?" we know exactly what the answer is going to be, which is what worries one. I am a strong believer in access by the medical profession to my medical records but what I do not like is the discovery, and I am told we were doing this and I did not know, that the Government are proposing to let all sorts of other people look at my medical records. I do not want a charter, I just want that not to happen under any circumstances and that is why, having a charter, okay, is a start maybe to give you access to check the accuracy. What we want is a basic stop, stopping the Government saying "Ah, that is a good idea, let's add them and them and them and add this additional data" and so on. Is that not what we really need to do?
Dr Forbes: One of the things that the Academy recommends is that we differentiate between the state and the Government. We allow the state to gather information about us, but we set up non-governmental authorities to hold that data so that the Government, if they want that data which is ours, has to apply and that makes it a public act, an accountable act and it is free to apply and ask for whatever it wants for whatever nefarious purpose, but then we get to know. That is the crucial thing. That is why I would use a charter: laying down these quite strict things within which everybody has to work and we understand what they are. As for trusting Government, most people are quite happy to let Government get on and do it; they do not really want to be bothered. That is a form of trust.

Q456 ***Lord Peston:*** Yes, but it is a negative form, is it not?
Dr Forbes: Compared with what?

Q457 ***Lord Peston:*** Compared with asking them the straight question "Do you trust the Government?" to which the answer is going to be "No".
Dr Forbes: With another system though; compared with what other systems, this is the one we want to trust.
Professor Sasse: Trust is not on or off, there are degrees and in a democracy it is absolutely right that you should not trust Government blindly. However, if the trust base between citizens and Government in general is very low, it influences people's behaviour. If you look at the number of people who are actually engaged in political processes, wanting to become involved in Government, if you look at voting figures and so on, those are also things that are connected to low trust in Government and that is really not desirable.

Q458 ***Lord Norton of Louth:*** Moving on to the RAE report's emphasis on the importance of public engagement in policy formulation, it stresses that it is very important that when discussing issues like privacy and related issues that there should be some arrangements in place that actually facilitate the involvement of citizens in policy formulation. What sort of arrangements? How feasible is it to give them that? I can see the principle but it is the operation of that principle. How does one actually achieve that?
Professor Sasse: In my view Government has recently been very fond of just holding consultations which are effectively rubber-stamping, opinion-poll-type things. I do not have a great deal of faith in those. If you contrast them then with more detailed investigations where people actually have a chance to discuss scenarios that personally concern them and then to relate their decisions, what is reported is quite different. It needs to be a more in-depth engagement. Say, for instance, you were deciding to change the voting procedures, you cannot just ask whether you would trust the Government to put in a proper internet voting system. You would need to show people what it actually means, what it would require them to do, what somebody else can see, where it would take place. It needs to be a meaningful consultation.

Q459 ***Lord Norton of Louth:*** I can see your point and clearly it links back to your point about trust because if people are involved in the processes, they discuss

privacy, it is their input and they feel they have had some say in it, then presumably they are going to trust that mechanism more. How does one have that wider consultation? If it is consultation, it is normally the usual suspects who respond, it is not people who are generally affected by these sorts of issues. How can we actually engage people in the deliberation so they feel they are involved and actually have a meaningful input?

Dr Forbes: This is a mass society problem and the problems that the technology brings also bring you some possibilities. I think the citizens are asked for data quite a lot and you could arrange that at certain times when a citizen is asked for data they are also asked other questions which would explicitly be about the consultation, would raise the kind of issues that people are concerned about and get their views on them, which can be very simply organised. Consultation used to be just insider groups frankly, but it is not necessarily now; in the last ten years there have been a lot of opt-in possibilities for consultation. However, there does need to be outreach work to give people the opportunity and to say you are going to collect this data but you are only going to do it if it is okay with you and these are the kinds of issues we are thinking about and these are the kinds of options that there may be and what are we missing and what do you care about? Some people do care a lot about their data and they will give you feedback and others will not and that is also data. Low voting figures can also mean that actually people think it is alright.

Professor Thomas: There is a real problem in helping people to understand the potential for a current act to cause future damage. I do not imagine that when the Netherlands, back before the Second World War, decided to include religious persuasion in their census data, they actually imagined they were going to be invaded by the Nazis and that it would be used to round up the Jewish population. Somehow you need to help people to look ahead. It is not out of the question that a future Government would decide that it was going to introduce a taxation regime that discriminated against people who had not looked after their health in the past, for example, and it is not out of the question that they would use information from Tesco store cards in order to gather that sort of data. I do not imagine that most people signing up for a Tesco store card have in mind that that is a risk that they are exposing themselves to. They might very well decide to sign up anyway, but it does seem right that something should be done at least to raise the level of awareness about the potential when you can store such huge amounts of data and search it so very, very easily.

Q460 ***Lord Norton of Louth:*** Does that not add to the problem? If you are going to consult with people, you have to inform them, they have to be informed, and in order to respond there is only so much information they can take in or would be interested in taking in, some of which might be quite technical. It is getting that balance.

Professor Sasse: Most important is when we are in systems design and we have techniques for this which we call scenarios. For instance, we write stories where the citizen, when being asked, can put themselves into that position and can then say "Yes, I would be happy if that happened" or "No, I would not be happy if that happened or if that happened to my child". There are techniques available for that and some of the companies that collect data are already using that in order to make sure these questions are really meaningful to the people answering them. There might still be an issue to engage a sufficiently wide range of the population and not just the internet literate, the YouGov users.

Q461 ***Lord Norton of Louth:*** Is there any example of this happening elsewhere that we could learn from in terms of that type of consultation?

Professor Sasse: The Netherlands is an example. What is happening there is that local government is a lot more involved in the decision-making process and they run these kinds of consultations and workshops locally and it then gets summarised and sent up.

Professor Thomas: There is a cultural difference across Europe. The countries which have been occupied by oppressive regimes in living memory tend to have a completely different attitude towards privacy.

Q462 ***Lord Woolf:*** Listening to you I am very conscious of two things. First of all you warn about the danger of data being collected and, secondly, you talk about things which could be done. What actually would you say is the practical thing that, if we are doing a report on this, should be done? You would not go so far, would you, or perhaps you would, as to say that nobody should collect data or retain data without a licence and the licence process would involve somebody scrutinising whether it has the safeguards in it that are needed? Or do you think the thing is going to police itself? If people do not look after data, their reputation will suffer. If Tesco were seen to be using the data they collect on their card for nefarious purposes, their reputation would be so damaged that it would be seen in the public reaction by not going to buy in Tesco.

Professor Sasse: Well the answer to that is that there would be a lot of people in a lot of parts of the country who would not even have that choice because they have no alternative. If you are in certain areas you might be very upset but you might effectively have no alternative.

Q463 ***Lord Woolf:*** I want to know what the practical things are that you three, as experts, would want to see. The only thing I have heard so far is that you would give extra powers to the Commissioner. That is really what is crucial.
Professor Sasse: Yes.
Dr Forbes: That is crucial, but also a digital charter, where you set out very clearly the expectations. You talk about a licence system. I would not recommend a licence system, but you need to generate a series of disciplines such that it is in the interest of the collectors of data to treat it well, to be open about it, to be accountable about it. What the drivers are for that will depend on which part of the operation you are dealing with and which kind of organisation you are dealing with. One of the things I would stress is the importance of reciprocity. If somebody gets my data, then why cannot I know everything I want to know? Why can I not be able to ask the questions I need to ask? At the moment, there is no provision for that. There is no requirement that somebody that collects my data for their purposes, for their benefits, has to respond to my questions. Once we get a proper relationship going, a reciprocal relationship, then you will get practice developing which serves the interests of both groups and not, as it is at the moment, mostly the interest of the data collectors and users.

Q464 ***Lord Woolf:*** Are you suggesting there should be a form of legislation or just in the form of promotion of good practice?
Dr Forbes: All of those things. The industry should be generating the standards as well as legislation from the top. We know that in terms of changing human behaviour you have to use a whole range of tools and you have to work out the best thing to do in each one of those.
Professor Thomas: Notification of loss, mandatory notification of loss or leakage of data, would be powerful. Shifting some level of liability, with a very low cost of applying for that compensation, onto the people who have to look after data would be a very powerful motivator and would cause Tesco to need to do the evaluation: "Is it worth keeping historic data? What is its value to us against the risk that it poses?" That is a practical thing. Looking further into the future, it might be possible to use the kind of digital rights management technology that the music industry is using to enable citizens really to own their own data so that when somebody asks for information from you, you could say "Yes, I will give you a licence to use that for these purposes and you can consult it six times and after you have done that, it will expire". The technology would permit that to happen; the DRM technology that exists would permit that to happen. It would be vastly too expensive and cumbersome to roll out at the moment but you could envisage that kind of thing happening in the future.

Q465 ***Baroness O'Cathain:*** I would just like to say this sounds fantastic and I can see that you have thought it all through and the Royal Academy of Engineering have, but has there been any analysis of the cost of all of these additional burdens that you are going to put on to companies, to Government, to the individuals? That is a real problem. Certainly in the realms of commercialism—and you have been going on about Tesco, so we might as well talk about Tesco—that would put a huge cost onto the operations of Tesco and make them uncompetitive.
Professor Sasse: Neither has there been any proper cost benefit analysis of the data that is currently being collected and used. For instance, there are examples where a company puts a registration form on the web for a particular service and when it comes to putting the telephone number down, 50 per cent of customers who started filling in the form drop out and do not complete the form because they think that if they put their telephone number down they are going to be called. The company says "No, no, no; we were not going to call, we are only using it for this particular purpose". So this misunderstanding is also a huge lost business opportunity and the actual benefit and cost associated with the data being collected is not understood either. If you put the two into balance, as we have always said, in a lot of cases collection would be quite limited because they would find out that the actual benefits are not really that much and in fact it can sometimes be counterproductive.
Professor Thomas: Proper design of systems would head off a lot of system failures and reduce the costs. At the moment it looks likely that the NHS Spine is going to fail simply because they have not addressed the privacy issues properly at the start of the process of doing design. As far as one can tell, there is still no technical specification for the so-called sealed envelopes that will protect the key data on the Spine. My best guess would be that actually the fundamental electronic patient record that lies at the heart of the national programme for IT in the Health Service will never be realised and that that huge expenditure with hindsight will turn out to have been wasted. A proper privacy analysis at the beginning could have enabled the NHS to get the systems that it needs in place by now with proper consent and adequate security.
Chairman: Dr Forbes, Professor Thomas and Professor Sasse, may I on behalf of the Committee thank you very much for attending and for the evidence you have given us. Many thanks.

WEDNESDAY 5 MARCH 2008

Present: Goodlad, L (Chairman); Morris of Aberavon, L; Norton of Louth, L; O'Cathain, B; Rodgers of Quarry Bank, L; Rowlands, L; Smith of Clifton, L; Woolf, L

Examination of Witness

Witness: MR PETER HUSTINX, European Data Protection Supervisor (EDPS), examined.

Q466 ***Chairman:*** Mr Hustinx, good morning. Welcome to the Committee.
Mr Hustinx: Good morning.

Q467 ***Chairman:*** Thank you very much indeed for coming all the way from Brussels. You are most welcome here. We are not being televised but we are being recorded, so I wonder if you would very kindly identify yourself for the record. If you would like to make a brief opening statement before we proceed to questions, please do so.
Mr Hustinx: Thank you. I am Peter Hustinx, I am the European Data Protection Supervisor. Shall I briefly explain what my mission is?

Q468 ***Chairman:*** If you could please explain your role as the European Data Protection Supervisor and how it relates to the work of the Article 29 Working Party established by the 1995 Data Protection Directive.
Mr Hustinx: With pleasure. I have been appointed by the Council of Ministers and the European Parliament jointly as from January 2004 to be the first European Data Protection Supervisor, which is basically a data protection authority as they exist in all Member States but now on the European level, and that fills a gap, quite frankly, because national law did not apply and before 2004 there was not an institution like this. I have three main roles, written out in more detail in the underlying regulation. The first is supervision, monitoring and ensuring compliance with data protection rules where they apply to the institutions and bodies, the Commission, agencies, the Council and Parliament, etc. That is about data processing by the institutions and bodies. The second role is consultation on legislation and policies with an impact on data protection. To be precise, whenever the Commission adopts a proposal for legislation with an impact on data protection it is under an obligation to send that proposal to me and my office for advice, which is then part of the discussion in Parliament and Council. I have developed the practice of being available for informal comments before that moment, and I give follow-up to the opinion in the discussions in Council and Parliament. So it is really consultation in the policy and legislative process as it proceeds. Thirdly, it is the role of co-operation, which is an under-statement because there is a soft co-ordination, long-term, promoting a consistency kind of co-operation—co-operation with national authorities and with the joint supervisory bodies in the Third Pillar. Much of this co-operation takes place in the context of the 29 Group you were referring to. I am a member of the 29 Group. Frankly, I used to be a member, before I was appointed EDPS, as the Dutch data protection commissioner.

Q469 ***Chairman:*** May I interrupt you there? Are you a member *ex officio*?
Mr Hustinx: I am a full member. If you read the text of the Directive it still referred, in 1995, to "an authority for the institutions", but that is now beyond any doubt. So I am a full member. That co-ordination then takes place in the context of the group. In practice, the legislative opinions I issue are mostly some time before the 29 Group endorses it, sometimes it specifies some points which are relevant, say, from the national group (?); sometimes I am second, sometimes we decide to just bring this together in one document. That is a question of timing, expediency or sometimes about the consensus. Overall, I am available and my staff is available on the ground on a daily level, and that is an advantage.

Q470 ***Chairman:*** How effective do you think the Article 29 Working Party has been in influencing policy and attitudes within the EU institutions and the Member States?
Mr Hustinx: Its impact on the policy-making is, I think, quite substantial. The 29 Group was designed as a mechanism in the Directive to provide for the so-called fine-tuning of the harmonisation approach. The Directive was a harmonisation instrument to make the intra-market (?) work better. It is not only a question of rules; it is also a question of practices. My activity since 2004 has certainly added, say, more substance, also, in terms of Third Pillar advice. That is a practice which has developed over the years. The Commission has welcomed it. I have offered it immediately, for the simple reason there is a lot of privacy in data protection issues around this, and it

does not make sense to be very particular about drawing lines. So we do both. In practice, it is 50 per cent Third Pillar related issues and, also, quite a lot of issues about the interface between private and public. The same applies, I think, to my role. We have evaluated the impact of the legislative council and consultation. In the First Pillar it is very visible, particularly in the role the Parliament is playing; there is co-decision and the Parliament, really, uses my input to prepare the response. In the Third Pillar it is somewhat different, although I am not very disappointed, but there it takes unanimity under current rules, which will change, as you know, next year, probably. It takes unanimity to come to a conclusion, and that is in many cases a decisive condition for, say, less than optimal results, and data protection is part of that problem. So, for instance (and we might come to that), I have issued three opinions on the Third Pillar framework decision, and I must say I am not very pleased with the result which is likely to be the end of the discussion in the course of this year.

Q471 ***Chairman:*** Can I ask: what are the obstacles to greater influence? Why are you dissatisfied?
Mr Hustinx: Part of it is the institutional arrangement, but as part of the Lisbon Treaty that is about to change, provided that is ratified by all Member States. However, if that happens (and I think the signs are positive) then this means there will be co-decision of Council and Parliament. There will be qualified majority or simple majority voting, there will be arrangements for adequate transparency in what is happening, there will be some oversight by the courts, and all that provides for the usual arrangements which lead to better decision-making on substance and, also, on respect for fundamental rights. Now, you made the point that the present arrangements also lead to less than the best conclusions in terms of effectiveness. Co-operation is something which needs to happen intergovernmentally, with inter-police and inter-justice co-operation—it is just, I think, a great practical need. However, due to these arrangements we see that sometimes necessary decisions are difficult. On top of that, if negotiations take place between police services and police ministers then the language of fundamental rights protection is not always welcome. So you need checks and balances to make this happen, and I think you are very much aware of this. So I am quite hopeful that this will be better next year.

Q472 ***Lord Rowlands:*** You have just mentioned that the Lisbon Treaty dismantles the Third Pillar. The UK have opt-ins and opt-outs in that arrangement.
Mr Hustinx: I have noticed, yes.

Q473 ***Lord Rowlands:*** Therefore, I presume, that opt-in and opt-out will also apply to the whole of your field, and that, in fact, the UK will not come under the same surveillance that you look eagerly towards.
Mr Hustinx: Allow me to go step-by-step. First, yes, the Third Pillar structure will be lifted—dismantled. So, basically, there is a holistic approach. Some of the details of the Third Pillar interest, of course, are still then part of the decision-making. So it is not entirely changing, but the basic structure means that for the role of the Parliament (and there is no opt-out in that case), if it comes to the Charter on Fundamental Rights, there are some opt-outs, and some of them are clear in the Treaty, but, of course, what has been accepted is the *acquis* which provides for the general principles of constitutional issues of all the Member States. The case law of the court is not likely to change as a result. I am not going to speak about the opt-outs, but I think for the analysis I was giving, and comments I will make, I do not think it will have a great impact. So it is relevant for all the Member States. What I would argue is that it is a very helpful improvement of the constitutional framework; that difficult issues of balancing different interests and ensuring fundamental rights, in the context where they are most needed—to balance protection at least. That improvement is important and it will also help me in making the points I have made before, and I will see, I think, better feedback.

Q474 ***Lord Rowlands:*** Do you anticipate that the new remit you will be obtaining as a result of the dismantling of the Pillar will apply to the United Kingdom, as much as those who joined up to the *acquis*?
Mr Hustinx: My remit is on the European level, but as to the consultation on new legislation I think I will see more impact of data protection safeguards after 1 January, assuming that is the date, if only because the Lisbon Treaty itself clearly specifies the need for Article 16 of the second part, the Treaty on the functioning of the Union, which provides for horizontal safeguards, which now even are going to apply to the Second Pillar, but certainly to the Third and the First. That will lead to the need to revisit some of this and it will then happen with the full involvement of the European Parliament. That means, probably, most of all, the Committee on Civil Liberties—which is the Committee on civil liberties, justice and home Affairs (that is an interesting combination)—are very much aware of the need to strike balances, because they do it all the time, and they are a keen supporter of adequate data protection safeguards. So my sense is we will see some improvement there.

Q475 ***Baroness O'Caithan:*** Mr Hustinx, you are reported as having said that "messages such as 'no right to privacy until life and security are guaranteed' are developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford". Can you elaborate on this, please?

Mr Hustinx: Yes, with pleasure. This was a statement I made in June last year, in the last month of the German Presidency as an invitation to the Portuguese Presidency. I was addressing some concerns which had developed over that period in Council. Some particular initiatives which I thought had great impact on data protection, anti-terrorism measures, were not prepared in a very satisfactory way, but, also, there was a trend of representatives of important Member States, as well as members of the European Commission, alluding more and more to the fundamental right to security (which is an important interest which I will judge, but is not a fundamental right of itself) and saying that there is a right to life and liberty, but the discussion of a right to public security was seen to be more than just a coincidence. This happened in the context of various informal ministerial meetings, statements and speeches in the European Parliament, and I felt it necessary to just give a strong signal about the existing arrangement. There was also the statement, I think, of John Reid, at the time, that it was important to perhaps reconsider the existing framework—the constitution of the Convention on Human Rights needed to be reconsidered. I found that worrying and it was that context which made me say what you have just quoted. Could I be more precise? The present framework relating to privacy and data protection but to fundamental rights in general do not deal with these rights as holy stones not to be touched, not to be excepted from under any circumstances, but they proceed in terms of balancing on the basis of very precise criteria. So the need for public security, for safety, is certainly a legitimate right, but you need then to specify what exactly is the purpose of a measure, and then the language. If it is necessary for that specific purpose and the law is clear—it is accessible, it is predictable and there are sufficient safeguards—then that measure is legitimate, but that then sets up, I would say, an agenda of tests which are to be met and demonstrated and verified, and this is how both courts in Luxembourg and Strasbourg (Strasbourg most of all, but both courts) proceed. This is what I apply in my advisory practice. The impact assessments which are usually part of these proposals are based on the same premise, but I am not always pleased by the way the impact assessment is done because the language is sometimes easy; we can say: "We think this is appropriate, this is effective and we think this is necessary; we think it is appropriate". So that was the background against which I have made the statement. It then led to a meeting in September with the Portuguese Minister of Justice and I think he recognised, basically, what I have said and that they were keen supporters of the existing system. So this was part of the public diplomacy, but sometimes it is necessary to give that signal.

Q476 ***Baroness O'Caithan:*** I find your answer quite staggering, actually, I have to say, certainly, on the basis that everybody says now that security of the state and the protection of human people in the state come as number one. This is what people in a democracy actually believe—that our security is much more important than privacy. After all, the threat to security comes from the unknown and threats to our privacy are more known, and it is the fear of the unknown, of course, which causes the problem. I am really flabbergasted, I have to say, because I reckon if you went on national television and made that statement people would say: "It's fine for them stuck in an office somewhere in Brussels to say they do not actually think security is that quantifiable and it is much better that privacy should come first". That is the way it would come across.

Mr Hustinx: This is not what I said. I would not subscribe to that summary. It is not a question of importance under other concrete circumstances; the question is: where do you start weighing what is legitimate? There is no doubt that in 1950, when this was concluded, and it has been applied in a list of cases, this is the way the court has measured. In very difficult cases in the 1970s, dealing with terrorism in Germany, the approach of the court was: there is no human rights-free zone; even the most invasive measures to protect security have to meet certain tests. That was the background. What is the problem is that, in certain contexts, it seems that governments find it difficult to comply with all the consequences of the safeguards, but that is part of the legitimacy. I was concerned by the fact that the repeated use of the language was suggesting things like: "Well, a different order from the one we have". If this was to apply to, say, a state which does not have any order, any security—a rogue state somewhere in the world—I would say: "Yes, let us first have some basic arrangements", but this was not the thrust of the discussion; the discussion was, in Europe and the United States: "How do we proceed with measures which are designed to protect security and which are stated to contribute to security but we do not have the discussion to convince that this is really necessary under the circumstances?" It comes in waves, if we see no proper evaluation of the effects of previous measures. So, no, this is not just an office or a university lecture; this is about practice. In order to get to say privacy is part of the basic security all citizens have a right to enjoy, if we want to protect

that society, we need to be specific. I am sure your Constitution Committee subscribes to that and it was against that background that I made my comment, and the comment was, of course, a public one, and that is sometimes very helpful to get points across.
Baroness O'Caithan: Thank you for that. The fact is, I reckon, we are probably all (well, I am anyway) thinking security equates with terrorism, and in fact that is probably the problem. To what extent do you think that the data protection arrangements within European organisations or systems that operate in the field of cross-border policing and criminal justice are providing a high level of protection of the rights of citizens in the context of those functions? Do you feel comfortable with them?

Q477 ***Chairman:*** Can I make an appeal, please, because we have a lot of ground to cover and not much time, for fairly brief questions and fairly brief answers? Thank you very much.
Mr Hustinx: I will try but this is a very difficult question. There is in the Treaty a policy goal which is framed in terms of an area of freedom, security and justice (they are grand) being developed step-by-step, presently, and rules which are less than satisfactory. You have referred to them. What we often see is that this goes by steps, and I am concerned by the fact that some of these steps do not include sufficient—quite frequently it happens—parallel tracking, parallel progress, and there are some clear examples of this. In my view we should see co-operation of law enforcement between the Member States (that is crucial; I subscribe to that entirely) and see things like data protection safeguards as part of the necessary conditions for building trust in these very relationships. This is not only citizens; this is also, quite frankly, the police and law enforcement versus law enforcement. So, to make this more effective, more efficient, more adequate, you need to integrate data protection safeguards. That is a tool to make things better. Unfortunately, this does not happen in practice. Unfortunately, decisions are made on the assumption that sometimes they will be followed by adequate measures, and the Treaty, in Article 30, now makes this a condition. So co-operation, subject to appropriate safeguards. A clear example is the framework for the Third Pillar. The Commission proposed this three years ago but it has not been adopted yet. Its scope has been reduced, its content has been diminished and in the meantime arrangements like the Prüm Treaty decision are pushed forward. That is another interesting example because (you may come to this later in the Committee) the Prüm Treaty was designed as a testing lab for seven Member States which had, more or less, the same experience. Before the first tests were really made, let alone evaluated, this was pushed up to a level of 27, and not with the parallel safeguards which you would expect, and I have made that point over the last year. This was part of the background of my comment on the mantra, and such like.

Q478 ***Lord Peston:*** You have referred to the Prüm Treaty.
Mr Hustinx: Prüm. It is a little place in Germany close to Luxembourg. It is like Schengen is, but that is Luxembourg. It is a little place where important treaties are concluded.

Q479 ***Lord Peston:*** Obviously, they are good concept places where important treaties are signed. You referred to it, and that takes us on to our favourite subject, DNA and mutual access to databases, and there are other provisions as well for the exchange of bio-information. Do you feel that this cross-border exchange of such information will one day have important effects on the lives of European citizens?
Mr Hustinx: No doubt, yes. No doubt. This applies to biometrics, DNA, fingerprints—all these things are extremely useful and interesting in police work. However, what is happening here is a huge infrastructure for setting up central databases in all Member States and providing direct access. That is not an easy thing; it involves 27 Member States providing direct access—it is an immensely complex task. What worries me is that we go from, in some cases, no experience at all with DNA to, in some cases, substantial experience with DNA. The United Kingdom is, perhaps, the world champion in DNA databases, but all this now in an environment where we have not thought sufficiently about how this should happen. So the Prüm Treaty was designed to be the testing ground and I am concerned that this is a less than satisfactory result. I predict (and I have stated repeatedly) that it will take a very long time before all this is implemented and we will see reports coming back in about this being delayed and we will hear the evaluation in the years to come. This is just a quantum leap in co-operation where we need to be doing this step-by-step and by learning from the experience. This is an important message, I would say. We see it all the time: measures are being piled up and they are not being evaluated. Sometimes there is an overdrive: "This is important; we cannot wait; we need to do this now", and the overdrive is the moment where risks are taken without sufficient evaluation because there is a perceived need to do something. Of course, we are not surprised to see a big deficit in implementation of decisions of the Council and, indeed, the anti-terrorism co-ordinator says: "A lot of my problems are that these decisions are not always implemented", and that meets my point that we need to avoid overdrive, to do this step-by-step, with a keen focus on, of course, getting results, and data protection is part of that. The Prüm

Treaty was an example of the scaling up of measures, and now, due to the fact that there is a lack of harmonisation as to the substantive rules—the rules in Germany, UK and France, let alone Bulgaria, Ireland, Denmark and Portugal, about DNA, who are not harmonised at all—if we start to access, to match, data on DNA, we will be confronted with all the complexity which arises from this diversity, and that is less than satisfactory. We will see in the courts arguments which could have been avoided in a more step-by-step approach. Let me make clear I am not against police co-operation; I am not against proper databases; I am not against direct access; I am not against biometrics being used, but it is just the overdrive and the problem of scale and the urgency which is the source of many problems—and, again, the lack of parallel tracks. If your staff check my advice in this context, I have made this point repeatedly.

Q480 ***Lord Rowlands:*** I think you may have partially, if not wholly, answered my question, and that is the cause of the delay in adopting the EU's Framework Decision. Is it that, in fact, a greater priority has been given to security as opposed to privacy, and/or, as you have already indicated in answer to your first question, it is institutional because it was in the Third Pillar and not the First?
Mr Hustinx: Institutional is an important dimension but there is also, I think, in my view, a not fully justified concern that accepting common standards in this area seems to be very difficult. I find that puzzling because these standards already apply under a Treaty which all Member States have signed and ratified; it was the 1981 Council of Europe Convention on Data Protection. Furthermore, they have been translated in detail, specified in the First Pillar. Many Member States have implemented this Directive horizontally (that means including law enforcement) but coming to an agreement on the full scope framework decision is extremely difficult. So one way to come to a consensus is to accept a narrow scope. What does this mean? I am sorry to say that the UK was one of those who made it very difficult to have this large scope, and that is part of unanimity. The narrow scope meant that only when data moved to another country the standards apply, but they do not apply from the moment data are collected until the moment they are used, as will be appropriate for basic, common standards. The consequence is that for all practical purposes, for a number of years, all law enforcement authorities need to be aware of country of origin and country of destination, and if they have a complicated case involving three or more Member States they will have diversity and complexity in every case. So all their databases will now have to track and trace where data came from. You can imagine, that is not very efficient. Had they accepted a wider scope it would have been better, but it has not happened. It was extremely difficult to come to specifications of the right of access to law enforcement data. So my hope is that if we can now start from a less than satisfactory result and go back on the basis of experience, with the involvement of Parliament and co-decision, that is probably then the only way forward. It is worrying because this relates to important areas of law enforcement co-operation. It is about, also, the interface between the Third and the First Pillar, and your investigation, say, on surveillance society is internationally based on these two concepts. I find it very disappointing.

Q481 ***Lord Morris of Aberavon:*** I hope I am not reading too much into your answer to the third question about harmonisation to precede access, but from what I gather it has an effect on my question. Is there not a balance between security and individual freedom? You are critical of the use of passenger names etc. What is the basis of your criticism? Is it because of the element of the invasion of privacy or is it because of something deeper—the threat to civil liberties and constitutional rights? It could be both, of course.
Mr Hustinx: Yes, it is both, but let me answer at two levels. First, the concept of data protection was developed years ago to provide protection not only for the right to privacy but (this is a quote from the Data Protection Convention) "and other fundamental rights and liberties", like non-discrimination, like free speech, monitoring how people read, how people express themselves, and fair process in a general way. There is a range of fundamental rights—the freedom to move is established. So it is not privacy in the strict sense; data protection is more inclusive. That is first. Second, applying the methodology I have applied for the last four years, which is based on the existing case law of the courts in Strasbourg and Luxembourg, I was struck by the deficiencies of the latest proposal on EUPNR. This was an example in which my opinion followed the 29 Group, and the 29 Group sums up 17 points on which it finds the proposal deficient, and I focus on four of them. The first, the major, is the legitimacy; the criteria of necessity and proportionality, and you look for the evidence in the proposal. There is hardly any evidence—it is very, very vague; it is anecdotal. The impact assessment does not provide any evidence on why there is a measure which is to lead to 27 central databases covering all airline passengers flying in and out of the European Union—all cases, no exceptions—a range of data. Why? Not to identify terrorists (because we have information on that), not to keep out people who are wanted; no, it is to collect information about everyone with a view to identifying possible risks and start to profile. That is a very, very far-reaching

proposal which leads to the question of effectiveness. There is some experience in the world that, in the case of the United States, was struck by the fact that the General Accounting Office of the Congress has raised lists of questions doubting the effectiveness of what is happening, and there is no evidence on all these levels. (See my opinion in detail for where this is supported.) So we say: "Shall we take a break to rethink this. Is this necessary? How are we going to deal with these data? Are they going to be exchanged?" That was the plan, and there will be a huge network of full surveillance of all airline traffic. Now, it is in that context that I made the comment (and it is at the end of the opinion) that this should be provided, in order not to end up in a total surveillance society environment. That was the context; the context was page 8, point 35 of that opinion—the conclusion. This is contrary to a rational legislative policy in which new instruments must not be adopted before those existing have been fully implemented and proven to be sufficient, and might otherwise lead to a move towards a total surveillance society. That is another big word, but that is the context. So, in my opinion, we should deal with important things in a serious and important manner, and this proposal, I think, is just not fully and seriously put. So it was probably submitted too early, and it could have benefited from that preparation.

Q482 ***Lord Morris of Aberavon:*** What you are saying is there should be a step-by-step approach?
Mr Hustinx: No, I am not arguing that we should move step-by-step to total surveillance, no, I am arguing that if a proposal like the one of EUPNR is made it should meet the test which applies to some huge operations, and that was a proposal of November. My opinion was given and within three months after that another package was proposed not only for all airline passengers but all passengers between now and 2015. So the waves of these proposals are profoundly worrying because they prevent proper analysis. I hope this analysis is going to take place and if this EUPNR proposal is not adopted before the end of December it will be subject to the new rules, and we will do this in co-decision with full involvement of the Parliament. That will be a very beneficial step in this case.

Q483 ***Baroness O'Caithan:*** In view of the remarks you made in December 2007 about the ways to regulate the use of Radio Frequency Identification, do you see specific legislation as the way forward for every new technological development?
Mr Hustinx: No, most certainly not. I believe that the existing framework, Directive 95/46, is, say, largely still appropriate. I do not subscribe to the idea that this is outdated. What we should do now, first, is improve implementation. I find that it is necessary to think about changing that framework to make it more effective, and we need to prepare for this. That was my position in June/July last year. One of the things we should look at is the interaction with new technology. RFID is an example of this new technology. It is not a little gadget; it is identified as a major new trend which is to develop something which is now referred to as the internet of things (?). We will be likely to be seeing all objects like, say, telephones, razor blades and food, and so forth, being equipped with these little tags and they will be communicating, they will be tracing our behaviour on a daily basis. Against that background I say that we need to implement the existing safeguards to the full. Part of that is using privacy-enhancing technology, using self-regulation—there is a list of things we could do—but just in case this is not sufficiently effective we should now provide for some vital additions in the focus of RFID applications. I mentioned three examples of measures we can take in that opinion, but is rather a signal that I see the existing rules as effective provided we use them effectively, provided we do have proper awareness-raising activities, that we have provided for mechanisms to enforce this properly and provided we use privacy technology to the full, and so forth and so on.
Chairman: Mr Hustinx, thank you very much indeed for joining the Committee and coming all the way from Brussels to give evidence. I very much hope the rest of your stay in London will be enjoyable.

Memorandum by Prof.dr. Bert-Jaap Koops, Professor of Regulation & Technology, Tilburg Institute for Law, Technology, and Society

1. The aim of this individual note is to provide input for the UK Constitution Committee's inquiry from a foreigner's perspective. I am not an expert in UK law nor familiar with all developments related to surveillance in the UK, but I assume that trends in the Netherlands are fairly similar to those in the UK. Hence, I hope my views on criminal law related to surveillance and technology in the Netherlands[1] are useful in the UK context as well. Moreover, I have conducted a comparative survey of constitutional rights and new

[1] As outlined in my inaugural lecture, B.J. Koops (2006), *Tendensen in opsporing en technologie. Over twee honden en een kalf* [Tendencies in criminal investigation and technology. About two dogs and a horse], Nijmegen: Wolf Legal Publishers, 55 p.

technologies in six countries,[2] commissioned by the Dutch Ministry of the Interior, and this study's findings may be useful for the Committee for comparative purposes. Since this note needs to be succinct, I only sketch the contours of my views, sometimes exaggerating for the sake of brevity and of argument. I start with an analysis of trends in technology and law (paras. 2–5) and then give some conclusions on the impact on the citizen-government relationship (paras. 6–10) and the role of constitutional rights (paras. 11–12).

2. Developments in technology, in particular ICT but also in biotechnology, have led to an enormous increase in data generation, processing, and storage. Not only are data stored in ever more databases (eg, Google, e-community sites, loyalty schemes, CCTV images)—a trend reinforced by legal instruments like the Data Retention Directive (2006/24/EC)—, but also, new types of data have appeared, such as location data (mobile phones), surfing data, identification data (RFID), and DNA data (like geographic ancestry), that traditionally were not generated or processed. Moreover, it has also become much easier to process and use data, through digitisation, automated recognition, data sharing, and profiling. Increasingly, data collection can also take place unobserved (aerial photography, miniature camera, directional microphones), using more senses than sight and sound (olfactory sensors, chemical "cameras"). Much of this is not new as such, but the scale of data increase and the combination of all developments lead to a truly qualitative increase in the data "out there" about citizens and their personal lives. And almost all of these data can, if legal conditions are met, be accessed and used by the government for law-enforcement and intelligence purposes.

3. Theoretically, the trend of increasing data accessibility is countered by likewise increasing opportunities to hide data: encryption, steganography, anonymisers, peer-to-peer file sharing, and Privacy-Enhancing Technologies (PETs) that use these techniques. In practice, however, PETs are little developed and even less implemented, and few citizens use hiding techniques. Some criminals and terrorists do use them, but there is little evidence that this has caused serious problems to criminal investigation to date; often, there are still sufficient alternatives for the government to gather evidence.

4. Adding together the trends of availability of data and hiding technologies, my conclusion is that the first trend seriously outweighs the second. The net result is that, even with the same investigation powers as formerly, the government is in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative but also qualitative.

5. The developments in technology are reinforced by developments in law. The investigation powers of investigation and intelligence services—at least in the Netherlands—have been greatly extended over the past decades. Starting well before 9/11, since the early 1990s, the legislature has broadened the powers for investigating telecommunications (both content and traffic data), observation, DNA forensics, and requesting data from citizens and businesses. Apart from using broader powers, surveillance is also taking place in earlier stages, focusing on prevention and early detection of crime (eg, preventative frisking, general identification duty). This results in broader groups of citizens being under surveillance: rather than investigating relatively few individuals on the basis of reasonable indications that they have committed a crime, more people, including groups, are nowadays being watched for slight indications of being involved in (potential) crimes. Thus, the "footprint" of criminal law and intelligence is slowly widening to cover more circles of society. This combined tendency in law (broadening powers, early investigation) is often technology-related, legitimising by law the use of newly developed techniques, but it also fits in a movement towards a risk-averse society (Beck) and a culture of control (Garland). In the Dutch context, I have concluded that criminal law has become a first resort in current society: for every risk and every problem, criminal law is being looked at as an almost natural instrument to address it. This constitutes a paradigm shift from the traditional role of criminal law as an *ultimum remedium*.

6. What are the implications of these trends for the citizen-government relationship? A first conclusion is that the balance of power has shifted. The technology- and security-related extension of investigation powers, reinforced by the quantitative and qualitative increase in data, has been primarily viewed by the legislature from the perspective of fighting serious crime—a battle of arms between police and criminals with technology as a primary instrument. What is often overlooked, however, is the net effect of this battle of arms on the average, unsuspected citizen, who is now under increasing surveillance without probable cause. Through the cumulative effect of diverse parts of surveillance, the citizen is becoming more transparent to the government, and citizens risk being in a weaker position than before if the government uses its increased power of knowledge in making decisions about citizens.

7. The shift in balance of power between government and citizens impacts the liberty and security of citizens. The move towards a culture of control and criminal law as a first resort carries with it increasing distrust: people may tend to a priori distrust strangers and unknown situations, and trust may therefore be decreasing

[2] B.J. Koops, R.E. Leenes & P. De Hert (eds.) (2007), *Constitutional Rights & New Technologies, A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States*, Tilburg, February 2007, 171 p. The Conclusion of this study is attached as an appendix.

as a primary basis in societal relations. It needs to be carefully researched what the longer-term effect is of such a trend on citizens' freedom. Conceivably, an attitude of distrust and the knowledge of being under constant surveillance has a chilling effect on citizens' freedom to develop themselves (fostering their identity) and to act uninhibitedly (fostering their privacy and autonomy).

8. An increased government power of knowledge over citizens is not necessarily wrong, since changes in society may warrant such a shift. However, it should be carefully argued that increased surveillance is indeed necessary, and empirical data are required to substantiate this. The developments sketched above are, however, often rather matter-of-fact; the whole process is piecemeal with small individual steps, which together constitute a giant leap. The policy and societal debates often focus on the individual steps rather than on the entire leap, and it is questionable whether the cumulative move towards surveillance is evidence-based and well-considered. A key recommendation for legislatures is to pay more attention to empirical underpinning of surveillance measures and their cumulative effect, to commission evaluation studies, and to use sunset clauses in legislation in case a measure does not show effect.

9. Also, more checks and balances are required. The increased government power needs to be balanced by additional checks, notably with more transparency requirements (citizens must know which data are being collected and processed for which purposes) and with enhanced audit and supervision. Independent authorities should regularly check whether the government uses its powers correctly and legitimately; the criminal court is no longer the primary instrument to check the execution of investigation powers, since many cases are not brought before the court, and alternative supervision mechanisms should be considered. Likewise, more information security is needed, since the police, in massive data collection, easily risks using incorrect or outdated data (see, eg, *Keegan v. UK*, ECtHR 18 July 2006). When data mining and profiling are used for criminal investigation and intelligence, mechanisms need to be in place to ensure careful application of profiles to individuals; citizens should not be confronted with government investigation merely because they fit a suspect profile.

10. In surveillance debates, data protection is a key element. To my view, the legal framework for data protection has become outdated. The assumption of preventing data processing as much as possible in order to prevent misuse of personal data is no longer valid in the current networked information society. Large-scale data collection and correlation is inevitable nowadays. Therefore, instead of focusing data protection on prevention in the data collection stage, it should rather be focused on decent treatment in the data usage stage. In other words, data protection is valuable not so much as a privacy-enhancing mechanism, but as a transparency and non-discrimination instrument.

11. This brings me to the final part of this note: the role of constitutional rights in the government-citizen relationship. Our comparative survey shows that constitutional values are important for technology policy and law, but in an indirect way: they often play an implicit role, through legislation that embeds and implements constitutional rights. In shaping the law and legal policy to face future, technology- and surveillance-related developments, constitutional values are urgently needed to help guide society through radical changes, particularly since it is hard to foresee in a timely manner which changes exactly are brought about by new technologies. It is important to closely study technological innovations that can be used for data collection and surveillance purposes and to assess these from a constitutional perspective.

12. In particular, various aspects of privacy, not in the least the protection of the home, the body, and correspondence, are threatened by new technologies. Since privacy is and will remain a core constitutional value, primarily as a key instrument in safeguarding citizens' liberty and autonomy in the democratic constitutional state, a critical assessment of the developments in technology and investigation powers as outlined above is required. Such an assessment could lead to a reconsideration of certain measures, a check on future broadening of investigation powers, or the establishment of substantial new checks and balances to counter-balance the increase in government power over its citizens.

4 July 2007

APPENDIX

Bert-Jaap Koops, Ronald Leenes & Paul De Hert (eds.), Constitutional Rights & New Technologies. A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States, report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, Tilburg: TILT, February 2007, Chapter 8.

8. Conclusion

Paul de Hert,[3] Bert-Jaap Koops,[4] Ronald Leenes[5]

8.1 *General*

This report offers the result of a comparative study commissioned by the Dutch Ministry of the Interior and Kingdom Relations. It contains six country reports, covering Belgium, Canada, France, Germany, Sweden, and the US. Every chapter studies the changes in constitutional rights and human-rights policy related to developments in ICT and other new technologies. The main focus is on the constitutional rights to privacy and data protection, inviolability of the body, inviolability of the home, secrecy of communication, and freedom of expression. As mentioned in the introduction, this report is a sequel to an earlier study carried out in 1999–2000 under supervision of Alis Koekkoek of Tilburg University.[6] The present study contains the same countries as the Koekkoek report. The central question in this report is to identify which developments have taken place in Belgium, Canada, France, Germany, Sweden, and the US with respect to constitutional rights and new technologies, in particular since 2000.

The authors of this report are not the same as the authors that contributed to the Koekkoek report. Their contributions are thus fresh and in the way their analysis consolidates the findings in the Koekkoek report, they add to the solidness of the academic preparations for possible Dutch reforms. The current authors have not restricted themselves to a description of the constitutional developments after 2000, so that all chapters can be read as independent descriptions of the constitutional systems of the six countries in relation to new technologies. All chapters contain a state-of-the-art analysis, with examples taken from the most recent constitutional developments.

On the basis of these analyses, this chapter will indicate general trends, signal some striking similarities and differences between the countries, and give a few recommendations for the Dutch legislator that can be distilled from these developments.

8.2 *General constitutional characteristics and developments*

8.2.1 Little constitutional dynamics as a general trend

A first sub-question dealt with in all the reports is general and concerns the nature and main characteristics of the six constitutional systems and possible changes to the constitutional system, in particular since 2000, for instance with respect to constitutional review, horizontal effect, or the influence of international law. The chapters show that there are several constitutional systems with almost no change, and a few with some dynamics. The US is an example of a system with almost no change. Their "rigid" constitution is very stable, and no significant amendments have been added or proposed. The Supreme Court has produced several relevant judgments that keep the interpretation of the Constitution up-to-date in light of technological developments. Belgium is an example of a country that used to be very static from a constitutional point of view, but has started to incorporate many changes. Its original 1831 Constitution has received several important revisions between 1970–93 in order to transform the Unitarian state into a federal state with a plurality of legislative bodies with distinct competences, and governments. In addition, the Constitution was enriched with certain fundamental rights relevant to this report in 1993–94 and in 2000. Moreover, the Court of Arbitration, operational in 1984 as an arbiter between the different legislative bodies, became a full Constitutional Court in 2004. Even in Belgium, however, technological developments have not been a primary trigger for constitutional amendments, and the fact that this country has been the most dynamic in constitutional change since 2000 among the countries surveyed in this report, indicates that new technologies have overall had little impact on constitutional changes over the past years.

[3] Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.

[4] Bert-Jaap Koops is Professor in Regulation & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.

[5] Ronald Leenes is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.

[6] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

The lack of profound constitutional changes in the countries surveyed has without doubt an institutional logic. Constitutions generally have a "rigid" status and are not meant to be amended or altered swiftly. This seems to be even more the case in federal systems with a delicate power balance between different governments. The US, for example, where the Constitution is still in function more or less in its original form, is a case in point. The Canadian fundamental rights, as formulated in the Canadian Charter of Rights and Freedoms (Part I of the Constitution Act, 1982), are extremely difficult to amend, since the consent of the Parliament is needed together with the agreement of seven to 10 provincial legislative assemblies representing more than 50% of the population.[7]

Another reason that none of the countries have undergone profound constitutional changes due to the emergence of new technologies, is that most constitutional rights, unlike Article 7 and 13 of the Dutch Constitution, are drafted in general terms broad enough to encompass new technologies. Freedom of expression and the right to secrecy of communications, for example, are usually worded in a technology-neutral way or, for instance in Sweden, with open endings like "and other technical recordings" and "or other confidential communications". Many country reporters stress the importance of technology neutrality in constitutional protection, given the usually complex process of amending the Constitution. At the same time, as Magnusson Sjberg warns, technology neutrality poses the risk of constitutional rights becoming very vague and thereby diluting constitutional protection. In that respect, open-ended formulations are to be preferred over overall abstract formulations.[8]

Still, the technology neutrality of most constitutional rights does not account wholly for the lack of dynamics. The chapters seem to suggest that developments in ICT and new technologies are often not looked at a from a constitutional or human-rights perspective, perhaps with the exception of general privacy issues. This seems to be especially the case for countries with older constitutions (Sweden, the US, and Belgium). These texts often tend to be smaller, more concise and less value-driven. The more pragmatic approach of Belgium contrasts heavily with the more principled approach of Germany and France, for instance in the area of biomedical technologies. It is not possible at this stage to assess these differences. One could also hold that the seemingly pragmatic approach in Belgium (with a Constitution that is very close to the Dutch) is inspired by the liberal value of freedom (eg, to sell one's organs or to alter one's body) that dominated most 19th-century constitutions.

The impression nevertheless remains: technology seemingly produces little constitutional dynamics. This is not to say that the Constitution is entirely dormant. In France and Germany, for example, constitutional rights play a fairly active role in debates. In Germany, this is due to the presence of many (post-Wold War II) value-driven constitutional rights, whereas in France, this results from more procedural basic rules, such as the rule that the legislator is obliged to define the guarantees to the exercise of fundamental rights and liberties. Hesitations by the legislator to fulfil this role account for most of the constitutional case-law produced by the French Constitutional Council in the area of new technologies.

8.2.2 The impact of international legal instruments

International human-rights treaties such as the European Convention of Human Rights (1950) and the UN International Covenant on Civil and Political Rights (1966) play an important role in the constitutional tradition of the European countries in this survey. In France, Germany, and Belgium, directly binding rights from international treaties, which are sometimes absent in the national constitutions, play a major role. The ECHR is more specific with regard to the possibilities for limitation, whereas the national constitutions tend to emphasise the existence of rights as such and usually do not go beyond the requirement that limitations have to have a legal basis.

Although not all of these European countries belong to the monist tradition (like the Netherlands), they are all eager to have cases decided in accordance with the case-law of the European Court of Human Rights. This situation stands in a striking contrast with the ethics of the US Supreme Court which, as a rule, does not refer to international treaties or case-law of foreign or international courts. Limitations to US constitutional rights do not resemble the European approach. The First Amendment with regard to freedom of expression omits every mention of the possibility to restrict this right, and the Fourth Amendment has its own particular requirements regarding limitations.

[7] See also H. Franken & A.K. Koekkoek, "The Protection of Fundamental Rights in a Digital Age", in: International Academy of Comparative Law, Brussels, Bruylant, 2006, at 1162. These authors discuss national reports from Canada, Denmark, Japan and the Netherlands.

[8] On the pros and cons of technology neutrality and strategies to deal with the trade-off between sustainability of law and legal certainty, see Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?", in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77–108, available at http://papers.ssrn.com/abstract=918746.

The open attitude in the European reporting countries also concerns acts and initiatives generated not by the Council of Europe, but by the European Union. Very often, ordinary legislation with regard to technological developments is enacted as a result of obligations created by regulations and directives (first pillar) or by decisions and framework decisions (third pillar). The position of the French Constitutional Council not to supervise national laws that implement European initiatives might be very problematic from a constitutional point of view with regard to third-pillar "laws" enacted without co-decision power of the European Parliament and without effective judicial control by the European Court of Justice.[9] However that may be, the omnipresence of the European law-maker in areas affected by technological change likely also accounts for the lack of national constitutional activity discussed above.

8.2.3 Constitutional review

We have already observed that most reporting countries have constitutional rights with an open texture that apply in one way or another to the use of new technologies. In addition, all reporting countries have a system of constitutional review, ranging from unlimited variants, such as the US (all courts without limitation in time), to more limited variants, such as France (only the Constitutional Council before or six months after adoption of the text of the law). The chapters do not allow concluding on the eligibility of a particular form of constitutional review. From a theoretical perspective, one could argue that the continuous development of technology does not allow a court to decide on the constitutional nature of a given law in too short a period of time, but this argument is not supported in practice by the French chapter, which shows an active constitutional court unhampered by the requirement to demand constitutional review within six months of enactment of a law.

What the chapters do show, however, is the importance of having one form of constitutional review or other in the first place. The Koekkoek report already concluded that all countries have constitutional review, and that the wish to formulate the Dutch constitutional rights in a more technology-neutral way was pointless if the Dutch prohibition of constitutional review (Art. 120 Dutch Constitution) were not abolished.[10] Particularly now that Belgium has recently opted for a quite broad form of constitutional review, the Netherlands have become even more isolated on the Western constitutional scene. Despite the recommendation of the Committee for Constitutional rights in the digital era[11] to install constitutional review and a bill to modify Article 120 Dutch Constitution, constitutional review is still not possible in the Netherlands. Significantly enough, the latter bill has been pending in the First Chamber ever since October 2004.[12] If the Dutch Constitution is to be amended to update the constitutional rights in light of new technologies—which seems urgently needed for at least the technology-specific rights of Articles 7 and 13—constitutional review should also be introduced in the Dutch constitutional system. Otherwise, the constitutional rights at issue risk having less effect in actual practice.

Having said that, it should be noted that constitutional review does not solve all problems. It allows the courts to keep the Constitution alive and to keep a check on the legislative activities of the legislature, but it can also function as a restraint on constitutional vitality. The US chapter clearly spells out a reverse evolution with regard to judicial activism: most of the expanding interpretations of existing rights are set back by the present Court with its more conservative composition. Effective human-rights protection therefore cannot rely solely on the eagerness of judges to apply constitutional principles to the society of today. Judges also need to work on the basis of constitutional texts and principles that guide them through their work, and hence, constitutions should have truly guiding principles and should not become too abstract or too general.

8.2.4 Horizontal effect

Technology is not an instrument specifically for governments; citizens depend on the use of technology at least as much. None of the constitutions of the reporting countries, however, contain any clause relating to the horizontal effect of fundamental rights.[13] Constitutional law seems to be devised as an instrument to regulate vertical relations and to protect citizen against governmental power abuses. It is clear that similar power abuses can occur by private actors, including businesses, but this has not had a clear effect on constitutional protection at large. Most reporting countries address the issue of horizontal effect by assuming in one way or another that it is up to the legislator to convert fundamental-rights protection into specific legal norms that

[9] See on this, P. De Hert, "Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs", in Apap, J. (ed.), *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement*, Cheltenham (UK), Edward Elgar Publishing Limited, 2004, 55–102.
[10] Koekkoek et al. 2000, op. cit. n. 4, p. 234.
[11] See section 1.1.
[12] *Kamerstukken I* [Dutch Parliamentary Series, First Chamber] 2004–05, 28 331, A.
[13] See also H. Franken & A.K. Koekkoek, *loc. cit.*, at 1155.

apply between citizens, for example in data-protection acts. On the basis of the chapters, it cannot be concluded whether the Netherlands should take specific action on this matter and open up constitutional protection in horizontal relations in a more direct way.

8.3 *Privacy*

8.3.1 General

The right to privacy is not explicitly mentioned in the Canadian, US, France, German, and Swedish constitutions, but it is recognised as being a part of the constitutional heritage in all the reporting countries. Belgium has, like the Netherlands, a general privacy right, albeit of a more recent date. The 1994 insertion of this right in Article 22 of the Belgian Constitution is remarkable, but in line with our observation above that constitutions in Europe tend to be sparing in possibilities to limit rights: it copies the general wordings of the right as we know it from Article 8, paragraph 1 ECHR, but omits the limitation grounds of the Article 8, paragraph 2 ECHR. When Belgium adopted the amendment, it was asserted that the right and its limits should be understood along the lines of the ECHR and its case-law. It is unclear whether such a use of supranational constitutional law at the expense of national constitutional law is beneficial. The chapters often suggest that proportionality is at the heart of constitution-related privacy debates, and it can therefore be suggested to incorporate the criterion of proportionality in future constitutional amendments.

Privacy in general is expressed in different terms and is constructed differently in the reporting countries. In Germany, where neither privacy nor data protection are mentioned in the Constitution, its source is Article 2, paragraph 1 and Article 1 (human dignity). In France, the source of privacy is not human dignity but liberty. Besides an implicit recognition by the Council in 1997, privacy was more explicitly recognised in French constitutional law in 1995-1999 as a part of the more generic right to individual liberty (Art. 66 Constitution) and rooted in Article 2 of the 1789 Declaration of Man and the Citizen: the right to liberty as an unalienable human right.

It is hard to assess the implications of these different expressions of the right to privacy and to put into question the formulation of the right to privacy as an independent right in the ECHR and in the Dutch and Belgian constitutions. It is neverthelss clear that the choice of Article 1 of the German Constitution (hereinafter: GG) as a source for the right to privacy is important for the strong position of the right to privacy in German constitutional law. The US chapter clearly demonstrates the weakness of privacy when it is not provided for explicitly in the constitution: privacy protection is built up and broken down by judges and can therefore fluctuate significantly.

The main constitutional provision in both Canada and the US where privacy is read into, is the provision protecting against unreasonable search and seizure. The chapters suggest that this right is formulated in terms that are perhaps too physical, but the cases quoted show that the wordings are (still?) open enough for the courts to apply them in a rapidly changing world. A crucial element in both rights is that they protect people, not places. This approach has significant advantages in a technology-driven world where traditional notions of place become blurred. In a world of Ambient Intelligence, "place" becomes something centering on people rather than on physical objects or geographical locations, since the surroundings change along with the people acting in them.[14]

Courts in Canada and the US also use the criterion of "reasonable expectations of privacy" to determine whether certain measures are unreasonable or not. Its application, especially in the US, seems rather tricky for privacy protection in a rapidly changing world where technology permeates everyday life. As technology develops, the "reasonable expectation of privacy" develops along with it, generally to the detriment of privacy as technology of itself tends to decrease privacy expectations.[15] An example is the Kyllo case in the US, where the Supreme Court used the criterion of a device being "in general use" to determine whether or not it infringed privacy;[16] as most technology applications tend to develop from limited, sectoral use to general, public use, the related privacy expectations at one point in time will become unreasonable. Hence, using "reasonable expectations of privacy" to face developments in technology poses the risk of a slow but sure erosion of privacy. Although the criterion is not wholly absent in the case-law of the European Court of Human rights,[17] courts and legislatures should be cautious in applying it in the field of technology law.

[14] See also infra, section 8.3.3.
[15] See Bert-Jaap Koops & Ronald Leenes, "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications & Technology Law Review 12* (2005) 1, pp. 115–188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.
[16] See section 7.4.2.
[17] ECHR, *Halford v. United Kingdom*, judgement of 25 June 1997, § 42. See also, generally, Sjaak Nouwt, Berend R. de Vries, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005.

8.3.2 Data protection

Recently, the role of data protection proper has received constitutional recognition in the EU Charter of fundamental rights of the European Union.[18] In the Charter, a separate right to data protection has been recognised apart from a right to a private life for the individual. The right to have personal data protected is, however, not explicitly mentioned in most constitutions of the reporting states, with the exception of Sweden and the Netherlands. Nevertheless, it is recognised as part of the constitutional heritage in all the reporting countries, and the incorporation in the EU Charter may be a sign of growing recognition for data protection as a constitutional right. Whether it will further develop as an autonomous right independent from privacy[19] remains to be seen: the chapters show that in most countries, data protection is (still) largely discussed in the context of privacy.

In Germany, the right to informational self-determination is a stand-alone right next to privacy. In France and Canada, the data-protection laws have a quasi-constitutional status. The French Data Protection Act is of a general nature. In Canada, the 1983 Privacy Act was designed to protect personal data in the federal public sector, whereas the 2000 Personal Information Protection and Electronic Documents Act was enacted to protect personal information in the private sector; only the first has quasi-constitutional value (it will trump other laws unless the other act addresses the privacy issues), the latter has the status of ordinary legislation. The 1995 EC Data-Protection Directive largely determines data protection in the European reporting countries.[20] Whereas Canada has responded to this initiative by enacting similar legislation, the US has refrained from adopting general ordinary data-protection legislation. In US law, however, some basic principles of data protection familiar to the Canadian and European regulations are absent. As soon as one gives data away or shares them, legal protection stops. The purpose-limitation principle, ie, the principle that data should be collected and processed according to a predefined goal or purpose, has not found firm ground in the US tradition.

All chapters show the overall importance of data-protection principles as yardsticks to measure new developments. Constitutionalization of these principles, in the line of the EU Charter, is therefore to be recommended. In that respect, it is worth mentioning that the protection of the EU Charter is more specific and more inclusive than the protection of Article 10, paragraph 3 of the Dutch Constitution. The latter does not, for instance, mention the role of the Data Protection Authority. Generally, one senses a reluctance of courts in many countries to apply data protection principles to their fullest extent. This is partly compensated by the activities of the national Data Protection Authorities.[21] In the line of the EU Charter, it can therefore be recommend to give these institutes constitutional recognition. Also, the pivotal role of the purpose-limitation principle in many debates, eg, the debate about privacy versus security, also suggests that this principle should be part of the constitutional codification of data protection.

Culture seems to be a factor of importance with regard to data protection. Although Sweden was the first state (after the German Land Hessen) to enact a national data-protection act (1973) and although Chapter 2, Article 3 of the Instrument of Government recognises that "every citizen shall be protected against any violation of integrity by automatic processing", Swedish constitutionalism is dominated by the notion of transparency and access to government information. Sweden therefore struggles with the main principles of the 1995 EC Data-Protection Directive and is now proposing a more US-like data-protection regulation that does not focus on prevention, but on data abuse. Given the strong influence of culture that the Swedish example chose, it can be recommended to the Dutch legislator that, when looking for inspiration for constitutional reform, he should be primarily oriented towards countries that largely share the Dutch human-rights tradition and cultural values. This is not to say that the Swedish development should be neglected: it can be questioned whether the European data-protection system, with its focus on a *priori* regulation of data collection and processing, can be upheld much longer in a world where data processing occurs in so many ways, to such an extent, and for so many purposes as it does today. Shifting the focus of legal protection to a *posteriori* regulation of data abuse might turn out to be a better strategy to protect individuals in the long run.

In all reporting countries, specific issues have determined the constitutional privacy and data-protection agenda. These overlap only partially, except with regard to the issue of balancing privacy and security, which has triggered significant debates and legislative activity in all countries. As a consequence of the September 11 attacks, many countries have adopted anti-terrorist laws, often but not always technology-related, that infringe on privacy or data-protection principles. The chapters show some resistance by the constitutional courts against overintrusive government powers, for instance in Germany, where the Constitutional Court has

[18] See http://europa.eu.int/comm/justice_home/unit/charte/en/charter02.html.
[19] As recommended by some scholars, eg, P. Blok, *Het recht op privacy*, Den Haag: Boom Juridische uitgevers 2002.
[20] See also H. Franken & A.K. Koekkoek, *loc. cit.*, at 1160.
[21] In France, for example, the Data Protection Act is acknowledged as law which guarantees a constitutional right, but the control of it by the Constitutional Council is weak. The Council only formally controls whether other laws respect the data-protection guarantees and principles established by the Data protection Act. In reality, control is therefore realised by the CNIL.

tied video surveillance in public places to the requirement that there are objective indications of dangerousness of the place to be monitored. Also, some cases have taken into account the proportionality criterion in dealing with proposed measures. In general, however, constitutional rights have not functioned to substantially limit or block legislative proposals to extend government powers to enhance security.

Besides "security versus privacy", the following themes have been mentioned in the chapters: video surveillance (France, Germany, Belgium), the use of camera's on highways (France), electronic surveillance or the e-bracelet (France), biometrics (France), the processing of location data (France), the impact of antiterrorism laws on other states (Canada), privacy competences of provinces in federal states (Canada, Belgium), access to government information versus data protection (Sweden), workplace privacy (Sweden), and genetic testing (Belgium, US).

8.3.3 Inviolability of the home

The inviolability of the home is covered explicitly in most constitutions, as such in the European constitutions except the French, and via the protection against unreasonable searches in the Canadian and US systems. Although these provisions have not triggered much debate in the reporting countries with regard to technological developments, two observations can be made.

The first regards the source of these provisions. Whereas French constitutional law considers the right to have the home protected as a component of individual liberty (Art. 66), most other systems identify privacy as a basic value underlying the protection of the home. This view certainly corroborates the observation that if there is an inner and outer sphere of privacy, then the home belongs to the most inner sphere (in the German term: Kernbereich) of privacy. It is not unproblematic, however. Indeed, the right to have the home protected is much older in legal history than the right to privacy, which was only recognised as such in twentieth-century constitutions. In the 19th century, it was therefore held that the right to property was at the core of the values underlying the protection of the house. It is unclear from a digital-rights perspective whether the right to inviolability of the home should be conceived as an independent right based on a plurality of values (liberty, property, privacy, etc) or as privacy specific right protecting not bricks but people, but this issue certainly merits a debate.

Second, linked to the foregoing, it appears that the current conception and wordings of the right to inviolability of the home is not technology-proof. The chapters identify problems with regular video surveillance in public places (the issues of homes is often addressed in this context), with satellite video surveillance, with RFID, with data relating to living conditions in houses (such as water and electricity bills), and with heat surveillance and other forms of scanning the home from the outside. Related to the latter, Article 13, paragraph 1 GG—"The home is inviolable"—has been complemented with a paragraph to allow the use of wiretaps, bugs, and similar equipment in homes for fighting organised crime "provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive". Similar issues in other countries have given rise to case-law. The Belgian Constitutional Court made it clear in 2004 that police competences to use bugs in houses needed to fulfil all the requirements of regular physical searches. In *Plant*, the Canadian Court accepted an inquiry of the police, who suspected drug cultivation, to the electric-utility company to have data on the use of electric power, because there was no trust relation between the owner and the company. The protection of the home in Section 8 Canadian Charter did not apply, because the electric reader did not reveal data on lifestyle but gave only primitive data. In *Kyllo*, the US Supreme Court saw a Fourth Amendment violation in the warrantless use of heat scans that monitored homes from the outside with devices not in general use. In *Teslin*, the Canadian court reached an opposite conclusion, arguing there was no reasonable expectation in heat that could be registered from outside homes; this technology did not reveal intimate details of lifestyle. This judgement seemingly contradicts the *Kyllo* findings but the Canadian Court left the door open to find a reasonable expection of privacy in relation to more sophisticated technology. An issue not yet addressed in case-law is to what extent the inviolability of the home protects against hacking into or searching, by means of a network connection, personal computers located in the home.

Both observations give rise to two questions that should be answered by constitutional legislators. First, are the spatial dimensions of terms such as "home", "search", and "illegal trespassing" technology-proof given the new means of monitoring the home from the outside in increasingly intrusive ways?[22] Second, what exactly is being protected by the inviolability of the home: the place or the people? Property, liberty, or privacy, or a combination of all these? It is important to take a stance on this, with a view to longer-term developments like domotics, which make homes "intelligent" and therefore more revealing of intimate life to outside snoopers, and Ambient Intelligence, where a personalised environment follows individuals as they move around, rather

[22] Cf., Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.

than that individuals have a fixed geographical basis for a private sphere in the form of their physical home. In the long run, the notion of "home" may need to be adapted itself to denote the personalised sphere around an individual rather than a fixed, brick-and-mortar place.

8.3.4 Inviolability of the body

The body is explicitly protected, like in the Netherlands, in Canada, Sweden, and Germany. The Belgian Constitution was amended in 2000 with a provision on the rights of children that includes protection of the body of the child. Other notions protecting the body are human dignity (France, Belgium), the right to life (Belgium), privacy (US, Belgium), and the privilege against self-incrimination (US)[23]. Canadian and German constitutional case-law suggest a high level of protection accorded to the body and to data related to the body. Canadian courts apply the rule that the closer something can be tied to the individual, the higher the expectation of privacy and the protection of the body. Thus, a handbag receives more protection than a school locker or a gym bag.

The right to have the body protected has not triggered many technology-related debates. Most debates, for example, about taking DNA samples, electronic monitoring of detainees, and using biometrics, have been conducted in the context of the general right to privacy and to ordinary data-protection legislation.

The notion of protection of the body is, however, particularly relevant for biomedical issues. Here, German and French law seem to be more principled and less pragmatic in their approach than the US, Sweden, and Belgium. The former systems let the notion of human dignity play a central role in these issues. In Germany, this right is rooted in the Constitution, whereas in France, it is recognised as a "Principe sentinelle (. . .) garants de principes constitutionnels" and has been firmly incorporated in the Civil Code since 1994 (*Bioethics Act*). Although it is not easy to determine whether the more principled approach of some systems or the more pragmatic approach of other systems is to be preferred, it is beyond doubt that, when endeavouring to involve constitutional rights in a more active way in biomedical developments, recognising human dignity can complement the right to protection of the body. It should, however, be noted that human dignity can be interpreted in a more or in a less liberal way. The current German interpretation, for example, prevents liberal abortion laws and gives heightened constitutional protection to the embryo, in contrast to the current European human rights framework.[24]

8.4 *Communication-related rights*

8.4.1 Secrecy of communications

The right to secrecy of communications is explicitly recognised at the constitutional level in Germany and Sweden. Contrary to the Netherlands, where letters, the telephone, and the telegraph are protected (Art. 13 Dutch Constitution), these countries use a sufficiently technology-neutral formulation: "the privacy of correspondence, posts, and *telecommunications*" (Germany) and "mail *or other confidential correspondence*, (. . .) telephone conversations *or other confidential communications*" (Sweden) (emphasis added). In Belgium and France, the secrecy of communications is not regulated at the constitutional level but by lower legislation; Belgium only has a constitutional protection of mail (letters). In Canada and the US, the secrecy of communications has been read into the constitutional protection against unreasonable search and seizure. In Canada, e-mail falls within the scope of this protection, albeit to a lower degree than letters, but in the US, constitutional protection of e-mail is still undecided. This is similar to France, where the protection of e-mail in ordinary legislation, as interpreted by the Constitutional Council, depends on the circumstances. In these countries, encryption of e-mail is likely a sufficient condition to invoke legal protection, but it is not a necessary condition: depending on other circumstances, unencrypted e-mail can also be considered secret (compare the *Weir* case in Canada).

As with the inviolability of the home, it is relevant to consider the exact nature of what is being protected: the communication itself, the place where the communication takes place, or the medium over which the

[23] This may also be the case in Europe, where the European Court of Human Rights found the administering by the police of an emetic (vomitive) to the applicant, who was suspected of having swallowed drugs, a violation not only of the right to be protected against inhuman or degrading treatment (Art. 3 ECHR) but also a violation of the privilege against self-incrimination (Art. 6 para. 1 ECHR). See ECHR 11 July 2006 (*Jalloh v. Germany*).

[24] See also, in general, comparing a utilitarian, a human-rights, and a human-dignity approach to addressing biomedical-ethical issues and warning against a too principled "dignitarian" approach, Han Somsen, *Regulering van humane genetica in het neo-eugenetische tijdperk*, inaugural lecture Tilburg, Nijmegen: Wolf Legal Publishers 2006.

communication is transported?[25] The US approach, similar to the Canadian approach, that the Fourth Amendment protects "people, not places" was established in the *Katz* decision on wiretapping. This remark referred, however, primarily to the place where the interception occurred: a public phone booth, arguing that people can have a reasonable expection of privacy even in a public space. This gives little guidance as to the core of the protection, but it is presumably closer related to protecting the sender or recipient of a communication and the communication itself than to protecting the medium transporting the message.

The German approach differs in this respect. The German Constitution protects the confidentiality of individual communications that depend on a third party for transmission; it principally covers all forms of mediated communication for the period of the transport. It is, hence, the channel that is protected rather than the communications as such. The French protection in ordinary legislation seems to be based on the same approach of transport protection. This "channel" approach has advantages in that it provides more legal certainty what kind of communications are protected, namely all communications transported across media that are protected as such, like the telephone. In the "communication" approach, the medium is neither a sufficient nor a necessary condition: protection has to be determined on a case-by-case basis, by looking at all relevant aspects of the communication itself. A channel approach is, however, more difficult to maintain as media converge. This is visible in Germany, where only individual communications are protected and not mass communications (such as broadcasts): this distinction is blurred now that communications infrastructures converge (eg, narrowcasting on TV infrastructures, broadcasting on the Internet, and types of communication on the Internet, such as blogging or communicating in large-scale but "closed" communities like Hyves, that are not easy to call individual or mass).

On the basis of the chapters, it can therefore not be recommended to choose either a "communication" approach or a "channel" approach, but it is advisable that constitutional legislators at least make an explicit and argued choice in this matter, to provide as much legal certainty as possible in this complex area.

Traffic data and data retention

A relevant issue—and a debated one in the Dutch context—is to what extent the constitutional protection of secrecy of communications covers traffic data (such as number, time, and—with mobile communications—location of a call). Generally, the reporting countries make a distinction between the content of communication and traffic data and find the latter less privacy-sensitive than the former. In Germany, traffic data fall within the scope of secrecy of communications (Art. 10 GG), but in other European countries such as Belgium and France, the protection of traffic data tends to be seen as part of the general right to privacy or data protection rather than as part of the secrecy of communications.[26] In Canada and the US, traffic data are treated—like the content of communications—in the context of unreasonable search and seizure, but with different outcomes: whereas the US denies constitutional, Fourth Amendment, protection to traffic data outright, Canada assigns some constitutional, Section 8, protection to traffic data, albeit to a lower extent than communication content. It is relevant to note that the latter distinction, made in the Lawful Access Initiative, is controversial in Canada, where scholars argue that traffic data can be just as privacy-sensitive as the content of communications.[27]

Given these varying constitutional approaches, it is hard to recommend how exactly traffic data should be protected at the constitutional level; perhaps it is ultimately a matter of choice to be made in light of the national interpretation of rights to secrecy of communications, privacy, data protection, and protection from unreasonable search and seizure. It should also be noted that, however varying the constitutional approaches may be, the material protection for traffic data does not necessarily differ that much in practice, since it is usually provided by ordinary legislation; the US ECPA, for example, offers more protection than the Fourth Amendment Katz standard.

[25] This is an as yet unresolved issue in the Dutch debate on adapting Art. 13 Dutch Constitution. The Committee on Constitutional rights in the digital era and the late-1990s bill to adapt Art. 13 opted for protecting communication as such, and therefore included face-to-face communication in its protection. Academic literature, on the other hand, particularly by several scholars of the Institute for Information Law of the University of Amsterdam, advocated a "channel" approach to protect the medium of telecommunications. See, for example, Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002. For a discussion of these varying approaches, see Bert-Jaap Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838–2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, at 277–286.

[26] Contrary to the European Court of Human Rights, which treats traffic data as part of the right to respect for "correspondence" in Art. 8 ECHR. See, eg, ECtHR 2 August 1984 (*Malone v. United Kingdom*) and ECtHR 25 September 2001 (*P.G. & J.H. v. United Kingdom*).

[27] This has also been argued by scholars in the Dutch context, opposing the position taken by the Committee on Constitutional rights in the digital era in this matter. See, for example, A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006, and the annotation by Egbert Dommering under ECtHR 25 September 2001 (*P.G. & J.H. v. United Kingdom), Nederlandse Jurisprudentie* 2003, No. 670, available at http://www.ivir.nl/publicaties/dommering/ehrm25sep2001.html.

A topical issue is data retention: the requirement for telecommunications providers to store traffic data for a certain period, as a measure to combat serious crime and terrorism. Significantly enough, this measure is only taken in Europe, with the 2006 Data Retention Directive;[28] it does not feature in the US anti-terrorism PATRIOT Act, and there are no proposals considering data retention in the US or in Canada. In Europe, France and Belgium had enacted data-retention legislation before the EC Directive. In France, the application Decree bringing into force this part of the Daily Safety Act was published in 2006, and ultimately approved by the CNIL as being constitutionally acceptable, given the limitations in the law of purpose-specification and duration. In Belgium, the implementing decree for Article 126 Electronic Communication Act is still in preparation. Germany and Sweden will have to draft implementation laws. From a constitutional perspective, it is relevant to note that a motion was rejected by the German Parliament to request the government to challenge the directive at the European Court of Justice,[29] but that several groups and individuals have announced to challenge the future German transposition law before the Constitutional Court.[30]

8.4.2 Freedom of expression

The freedom of expression is an important constitutional rights in all reporting countries. The scope of the right differs, however. In France, Sweden, and the US, the right focuses on the *expression* or *communication* of thoughts and opinions. Canada has a more encompassing right, covering also the freedom to hold thoughts and beliefs; Belgium is similar in that it creates the freedom of expression along with the freedom of worship (Art. 19 Belgian Constitution). Germany also stipulates a constitutional right to gather information, to stimulate the forming of thoughts and opinions.

Despite the overall importance of the freedom of expression and the largely similar culture in the reporting countries to favour openness and public debate over censorship, each country distinguishes certain types of speech that are excluded from protection. Several of these are shared by most countries, such as—in the US terminology—"true threats", defamation, and child pornography (in all reporting countries), and hate speech (in all except the US). Other categories are more specific for certain countries, such as political speech (banned in Canada in the 20-hour period preceding the closing of polls, given the vastness and time zones of the country), court proceedings (which in certain cases cannot be published in Canada), and commercial speech (which has a lower standard of protection in the US). For virtual child pornography, it is noteworthy that a US law banning this was struck down as unconstutional; the constitutionality of a subsequent, more strictly formulated but functionally equivalent, criminalisation has so far not been decided in court. In the other reporting countries, several of which have also criminalised virtual child porn in the wake of the Council of Europe's Convention on Cybercrime, the constitutionality of these prohibitions does not seem to be an issue.

Particularly relevant in the context of this report is the freedom of media that express or transmit opinions. Article 25 of the Belgian Constitution is restricted to freedom of the press, which tends to be associated with the printing press, and courts are reluctant to interpret this to cover new media. The US First Amendment also only mentions freedom of the press, but this is interpreted much more broadly than in Belgium, and there is no debate that the right is formulated in too technology-specific a way. The German Constitution, in Article 5, mentions the freedom of the press and the freedom of reporting by means of broadcasts and films, thus distinguishing the press from audiovisual media. Given a similar distinction in French ordinary legislation, the Internet has triggered a restructuring of French media law, which now has a general category of "electronic public communications", which is divided in two sub-categories: "audiovisual communications" (subject to the Freedom of Communications Act), and "on-line public communications" (subject to the Trust in the Digital Economy Act). Canada and Sweden have no problems with new technologies, since they use open-ended formulations: "and other forms of communication" (Canada), "and certain like transmissions, (. . .) and other technical recordings" (Sweden). Nevertheless, given the fact that Swedish constitutional protection of freedom of speech is spread across two constitutional laws, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, an inquiry is on-going to merge these laws.

The Internet raises several questions with respect to the freedom of expression. A primary topic is the categorisation of bloggers. On the one hand, they serve a purpose very similar to journalists in the printed press, by fostering the collection and spreading of information, ideas, and opinions, and therefore may well, in the longer term, turn out to be equally valuable for the public debate as traditional media, or perhaps even more valuable. On the other hand, on the Internet, everyone can start a blog and call herself a journalist. The reporting countries are tentatively coming to terms with defining bloggers. In Belgium, the criterion of "everyone who directly contributes (. . .) information aimed at the public via a medium" has been formulated

[28] European Directive 2006/24/EC of 15 March 2006 on data retention.
[29] http://dip.bundestag.de/btd/16/016/1601622.pdf.
[30] http://www.edri.org/edrigram/number4.10/dataretentionde. Outside the scope of this survey, but relevant to note in this respect, is the case brought before the Irish High Court against the Irish government by Digital Rights Ireland, challenging the Irish data-retention law and the EC Directive as unconstitutional. See http://www.digitalrights.ie/category/data-retention/.

to trigger applicability of the Act on the protection of journalistic sources, thus in principle covering bloggers as well. In Canada, courts tend to apply a broad definition of journalism as well in relation to new media.[31] In Sweden, a more material criterion is used, namely that information be "of importance to the public debate" in order to be protected by the freedom of expression;[32] this allows courts to assess bloggers—and other expressers of opinions on new media—on a case-by-base basis in light of the rationale of the constitutional protection. With converging media, this seems a more sustainable approach than a media-centered type of protection.

Other interesting Internet-related issues with respect to the freedom of expression are the distinction between static and interactive websites (in Sweden, only static websites fall within the scope of the Fundamental Law on Freedom of Expression), the liability for hyperlinks that link to prohibited speech (Germany: no liability because the hyperlinker aimed at faciliting people to form an opinion; France: liability because the hyperlinker had explicit knowledge of or advertised the linked content), the liabiliity of ISPs (eg, in France and Canada), and filtering systems (eg, in Canada). Also noteworthy are the activities in France and Belgium for the protection of minors on the Internet.

On the basis of the reports, it can be recommended that the freedom of expression—possibly strengthened by the freedom to gather information and to hold beliefs and opinions—is formulated in a sufficiently media-neutral way. An enumeration of media with an open-ended formulation—like the Canadian "and other forms of communication"—seems particularly apt to strike a balance between legal certainty (for media that should be protected in any case) and technology neutrality (for media that may also need to be protected, perhaps through future technological developments). Given the increasing convergence of media and the rise of new ways of expression, such as blogging, that blur tradiational concepts like "journalist", it is also useful to consider including, besides or instead of the mentioning of media, a material criterion, such as "of importance to the public debate", that judges can use to decide whether in a concrete case a communication serves the values underlying the freedom of expression.

8.5 *Other and new constitutional rights*

The chapters have also mentioned several other constitutional rights as being affected by new technologies. Apart from the right to anonymity, which all reporters touched upon as it closely relates to both privacy and freedom of expression, and which we therefore treat separately in this section, no general conclusions can be drawn from the chapters, since the reporters were asked to focus on the privacy-related and communications-related rights and to go into other rights only as far as time and expertise were available.

8.5.1 Right to anonymity

Although anonymity is a topic of debate in all reporting countries, none of the countries knows a general right, constitutional or otherwise, to anonymity. It is, however, often a subsidiary or a derivative of constitutional rights. There exists, to some extent, a constitution-related right to anonymity in the context of privacy (in France), data protection (in the form of the right to informational self-determination, in Germany), the secrecy of communications (in Germany), free speech (in Canada and the US), and the right to individual liberty (which, in France, includes the freedom to come and go anonymously). This right is far from absolute: numerous exceptions are made, such as a legal obligation for bloggers to inform the hosting provider of his identity (France), a ban on equipment that obstructs caller-identification in telecommunications (Belgium), and a prohibition of anonymous political advertising (Canada). Also, discussions about revealing the identity of unknown or pseudonymous Internet users alledgedly infringing copyright or committing a content-related crime online, can be witnessed in all countries, often allowing the lifting of anonymity of the purported offender. A conclusion that can be tentatively drawn from this overview is that anonymity tends to be protected in most countries as a not unimportant value, also at the constitutional level, but that infringements of anonymity are generally easily accepted. It is therefore not possible, on the basis of the chapters, to conclude that a "right" to anonymity exists; rather, it plays a role as a value in the context of several other constitutional rights.

8.5.2 Various

Various constitutional rights and issues are mentioned in the chapters as being potentially affected by new technologies. We give a brief overview here.

[31] Jason Young, communication at the 1 December 2006 workshop.
[32] Cecilia Magnusson Sjberg, communication at the 1 December 2006 workshop.

The freedom of assembly is possibly relevant for on-line demonstrations or virtual sit-ins, although a lower court in Germany declined applicability. Equal treatment (Art. 10–11 Belgian Constitution) was an issue in Belgium when the Official Journal (*Belgisch Staatsblad*) was transformed into an on-line publication, impacting the accessibility of the journal in an unconstitutional way. Computer games raise questions about the applicability of personality rights, such as portrait rights, and the freedom of art; a German lower court held that a computer game could claim the constitutional right to freedom of art, but the appeal court found that even so, a celebrity's consent was needed to use his name in the game. In the United States, a right to experimental, potentially life-saving, medication was invoked even if the drugs had not passed all tests for FDA approval. In France, the right to be forgotten is mentioned for underage offenders.

In the criminal-law context, the criminal legality principle (no crime without prior law, Art. 12 Belgian Constitution) is relevant in that it requires precise law-making, so that citizens can foresee what is punishable and how they can be investigated. In the Belgian Computer Crime Act, the formulation of "any other technological means" was used in an attempt to make the description technology-neutral. This meets the legality principle on the face of it, since all "technical" crimes are covered, but at the same time, foreseeability is not guaranteed with such an open ending. Also in the criminal context, in the US, the privilege against self-incrimination (Fifth Amendment) is relevant in relation to technology, for instance in the context of a power to compel citizens to hand over encryption keys. Brenner argues that such a power would violate the Fifth Amendment unless the key (or password) was reduced to tangible, recorded form. Saliently enough, such a power, which has not been enacted in the US, does exist in France and Belgium, but in these countries, the power to force suspects to decrypt has so far not been challenged as infringing the privilege against self-incrimination.[33]

In the context of electronic government, various issues spring to attention. Notable first of all is the right to access public information, which is a constitutional right in both Belgium and Sweden. Both use the term "document". In Belgium, this has been interpreted broadly to cover all kinds of documents regardless of the storage medium, whereas in Sweden, the term "recording", used alongside "written or pictorial matter" in the definition of "document", refers to electronic documents. "Recordings" in Sweden can be ready-made (such as e-mail messages) or compilations (like merged data bases); compilations only fall within the scope of the right to access public information if the government can make them accessible "using routine means". In Sweden, also the storage and deletion of official electronic documents has been called attention to in the context of the right to access public information.

Another relevant rights in the context of e-government is the right to vote. In Belgium, the law was adapted in 1998 to allow voting machines, without debate; in the US, a few civil-law suits arguing that flawed voting machines violated their right to vote were denied. E-voting has been discussed and briefly experimented with in France as an alternative to distance-voting.

Finally, a fundamental issue is raised in the Swedish chapter outside the field of human rights. The power to enact laws is constitutionally attributed to the legislator (the Riksdag, and sometimes the Government or by delegation another public authority). The increasing use of computer-assisted and computer-executed legal decisions, notably in the field of administrative law, raises the question whether and to what extent the programs used for these decisions, in which rules are embedded, should be seen as enacted laws. After all, the legal rules of law proper are not trivially translatable into technical, computer-logical rules, and hence, programming constitutes a degree of autonomous rule-making. This requires a check on the conformity of the resulting program rules with the legal rules and on the constitutional authority underlying the technical rule-making process. Related to this is the issue in Sweden of the distribution of competence between local and central authorities: if administrative decisions are largely the result of centralised information systems, the constitutional task of local governments to take indivdidual administrative decisions is at risk.

8.5.3 Conclusion

Although no general conclusions can be drawn from this brief overview, two observations can be made on the basis of the mentioning in the chapters of other rights. First, the challenges that new technologies pose to constitutional law are wide-ranging and go deeper than merely the occurrence of technology-specific formulations in constitutional provisions. The issues mentioned range from traditional, age-old constitutional rights like the freedom of assembly and the right to vote to more recent or new rights, such as the right to access government information and the right to be forgotten. What is more, they also relate to constitutional issues outside the field of human rights, such as the division of power within the government.

[33] The privilege against self-incrimination is not always recognised at the constitutional level in European countries, but it is at the core of the constitutional right to a fair trial as interpreted by the European Court of Human Rights, since its first acknowledgement in ECtHR 25 February 1993 (*Funke v. France*).

Second, despite the wide range of issues touched upon, the issues signaled by and large relate to developments in the near rather than the distant future, and they tend to involve ICT rather than other new technologies. This may well be caused by the background of the reporters, all of whom have a track record in the field of ICT law in particular, but it could also be an indication that biotechnology and genetics, nanotechnology, and the convergence of nano, bio, information, and cognitive sciences (NBIC) have as yet caused little discussions in relation to constitutional rights. The long-term impact of these developments on fundamental issues, for example, whether cyborgs and robotics necessitate a rethinking of the concept of the bearer of constitutional ("human") rights, or the effect of NBIC on legal notions based on the concept of free will, has to our knowledge not been discussed in any detail in literature or in constitutional-policy debates.

8.6 *Conclusion*

New technologies challenge constitutional rights. This is particularly visible in the Dutch context, where the technology-specific formulation of several constitutional rights necessitates an adaptation of the Constitution. In the countries covered in this report, however, the text of the Constitution itself is hardly at issue. In some countries, a few adaptations have been made to bring the formulation up-to-date in light of new technologies, but no such adaptation has occurred since 2000, and no need is currently felt to adapt the Constitution—with the possible exception of the Belgian freedom of the "press". Generally, constitutional rights are sufficiently technology-neutral, because they are abstractly worded or use open endings (notably in Sweden), use guiding principles like a general right to personality (Germany), or are kept up-to-date by constitutional or other courts who can interpret the rights by deviating from a literal reading (US, Canada). Constitutional review is also, in varying forms, a primary feature of all constitutional systems covered in this report that explains the lack of need to modify the constitution itself.

Besides a lack of constitutional amendments, a general trend is perceptible of low constitutional dynamics. Some countries, notably Belgium, have seen a relatively vibrant constitutional activity in the past few years, with a full-blown Constitutional Court as a result, but in most countries, constitutional rights do not seem to play a key role in debates over new technologies, at least, on the face of it. A second look at many of the issues covered in this report shows that constitutional values related to privacy and freedom of communication do feed technology-related policy, legislation, and case-law, but often without reference to specific constitutional rights. In other words, constitutional values are important for technology policy and law, but in an indirect way: they often play a role in an implicit way, and through other, non-constitutional legislation that embeds and implements constitutional rights.

This is hopeful, because new technologies pose challenges, if not to Constitutions as such, to all areas of the law. In shaping the law and legal policy to face future, technology-related developments, constitutional values are urgently needed to help guide society through a process that will certainly bring radical changes, particularly since it is hard to foresee which changes exactly will be brought about by new technologies. Constitutional rights are core values that define what human beings and society are and should be. Therefore, even if constitutional rights are far from dormant, legislatures and policy-makers would do well to more explicitly refer to constitutional rights in their activities, and to create an environment in which constitutional rights can flourish and guide society along.

For the Netherlands, this means not only that several constitutional rights that are currently worded in a technology-specific way should be adapted, but equally or perhaps even more importantly, that a form of constitutional review should be created that allows constitutional rights to mature and work in practice.

July 2007

References

Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002.

H. Franken & A.K. Koekkoek, "The Protection of Fundamental Rights in a Digital Age", in: International Academy of Comparative Law, Brussels, Bruylant, 2006, pp. 1147–1164.

P. De Hert, "Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs", in APAP, J. (ed.), *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement*, Cheltenham (UK), Edward Elgar Publishing Limited, 2004, 55–102.

A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

Bert-Jaap Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838–2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, 335 p.

Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?", in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77–108, available at http://papers.ssrn.com/abstract=918746.

Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.

Bert-Jaap Koops & Ronald Leenes, "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications & Technology Law Review 12* (2005) 1, pp. 115–188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.

Sjaak Nouwt, Berend R. de Vries, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005.

A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006.

Han Somsen, *Regulering van humane genetica in het neo-eugenetische tijdperk*, oratie Tilburg, Nijmegen: Wolf Legal Publishers 2006.

Examination of Witnesses

Witnesses: Professor Bert-Jaap Koops, Tilburg University Institute for Law, Technology and Society (TILT), the Netherlands, (via video link), and Dr Lee Bygrave, Associate Professor, Faculty of Law, University of Oslo, examined.

Q484 ***Chairman:*** My Lords, can I welcome to the Committee Professor Koops. Can you see us from your area in the Netherlands?
Professor Koops: Yes, I can see you. I can hear you, although the volume is not very high.

Q485 ***Chairman:*** We will speak up clearly. We can see you and you are very welcome to join the Committee. Thank you very much indeed for doing so. Also, welcome to Dr Bygrave, who is here in person, who has come to us from Norway. Could I ask, because we are being recorded, although not televised, if you could each give your name for the record and your position? If you would like to make a brief opening statement before we start questions, please do so.
Professor Koops: My name is Bert-Jaap Koops, I am a Professor of law and technology at Tilburg University. I do not particularly want to give an opening statement but I think I should say that I am a foreigner with not too much knowledge of the United Kingdom and so my evidence will be as an outsider looking at it from a distance.
Dr Bygrave: I am Dr Lee Bygrave; I am an Associate Professor at the Faculty of Law, University of Oslo. As you can probably hear, I am not Norwegian—originally I am from Down Under—but I have been based in Norway for the last 15 years, and am reasonably well-experienced with data protection law and practice in Europe.

Q486 ***Chairman:*** Thank you. Could I address the first question to Professor Koops, please, and do come in afterwards, Dr Bygrave, if you wish. Professor Koops, the United Kingdom is often said to have the most extensive surveillance of any liberal, democratic country. From your knowledge of other countries, do you think that assertion is valid? If you do not, could you give a more nuanced assessment of British surveillance?
Professor Koops: It is hard to say that the UK is a surveillance society more than other liberal, democratic societies at large because there are many aspects of surveillance. There are certain aspects, particularly, for example, the national DNA database, where the UK has probably gone further than any other country that I know of. However (and I am not sure it is a good example), on identity cards and identity numbers, I think, the debate you are having on identity cards shows that you are a bit wary of identity mechanisms as a surveillance measure, whereas many other countries have long ago introduced identity cards and identity numbers without any discussion. Another example could be wire-tapping, where, in Europe, Italy and the Netherlands have by far the highest incidence of wire-taps, probably—certainly in the Netherlands—much more than in the UK. It is difficult to give exact numbers. The entire system of surveillance measures is a sum of measures, and you have more of one thing and less of something else. We wire-tap more that

means we infiltrate less. If I can give an overall picture, I think the UK is going far and fast; it is more extensive than most other liberal countries but there are certain aspects on which it certainly is not so much.

Q487 ***Chairman:*** Do you think these issues are taken seriously in the parliaments and national governments and institutions of the European Union?
Professor Koops: I am afraid I should say not always. Perhaps I should say more often it is not really taken seriously, from my knowledge, but there are exceptions. For example, in Germany, the Government and the Parliament is sensitive to privacy issues and to constitutional rights, but many other countries are a bit lax. Yes, they do pay attention to privacy but they do not really feel privacy and other constitutional rights are really important, and they do not really do something with it.

Q488 ***Lord Rodgers of Quarry Bank:*** I have two questions, both to Professor Koops as well as Dr Bygrave. Are the effects of surveillance—we are talking about the United Kingdom—detrimental to civil liberties, human rights and the protection of privacy? I wonder whether you have any evidence or examples to illustrate your reply.
Dr Bygrave: I want firstly to just endorse what Professor Koops said in relation to the previous question and elaborate on one aspect there. If you look at the Scandinavian countries, you have had, for example, national personal identification systems in place from the 1950s and 1960s without very much discussion at all of the possible impact on civil liberties—indeed, the systems were just accepted as sensible, administrative measures—and yet that sort of initiative creates a lot more public debate here in the UK and, indeed, many other jurisdictions. So this, again, just shows that assessing the overall surveillance level of any one society, and comparing it to another, is a very difficult and treacherous exercise. At a street level, when I am wandering around London, I do not really notice any difference in surveillance from another European country, except, obviously, for bigger numbers of surveillance cameras. That is what is happening at street level, but I would say that equally if not more importantly is what is happening beyond street level, and there it is often very difficult to get accurate information as to what exactly is happening. It is also worth noting that in one of the most extensive comparative studies of surveillance levels and the regulatory regimes around surveillance, carried out in the 1980s by a Canadian professor, David Flaherty, the conclusion was that Sweden was the closest to being a surveillance society. That was a study published back in 1989. Professor Charles Raab is well acquainted with that study, so he could elaborate on it for you later. Flaherty's conclusion that Sweden was the most surveilled society was built, largely, around the very existence of this national personal identification number and the extensive data-matching it facilitates. The UK, by the way, was included in that comparative assessment. Regarding detriment, obviously there is detriment to privacy if you regard detriment in terms of reduction of privacy. Surveillance, by its very definition, involves a reduction of privacy. The degree to which surveillance has a debilitating effect on one's perception of freedom and how one actually acts is more difficult to gauge. Bentham's Panopticon, as you all know, was premised on some knowledge of the control system in place, but that knowledge is often not present with surveillance measures, so people can, nevertheless, go around thinking they are free even though they are really in some sort of aquarium.

Q489 ***Lord Woolf:*** Do you think that the differences that exist between the UK and other continental countries are partly because of our lack of a written constitution, which would provide greater protection for the privacy of the individual and controlled data collection? I address that to both professors, and perhaps you, Dr Bygrave, would answer first.
Dr Bygrave: Well, it all depends on what is in the constitution, of course. Constitutional provisions for the protection of civil liberties can be formulated in many different ways, some of which provide, in effect, really just symbolic protection for the liberties concerned. It also depends on the type of judicial review that can be carried out on the basis of a constitutional protection. However, it is clear that if you look at, say, the Federal Republic of Germany, which arguably has the strongest protection for personal data in Europe, that constitutional platform has been very, very important for the case law of the Bundesverfassungsgericht in curbing, particularly, the latest spate of surveillance measures being issued by the interior ministry in the Federal Republic, and, also, at Länder level. I am not sure if you are familiar with the decision handed down just last Wednesday, 27 February.

Q490 ***Lord Woolf:*** No.
Dr Bygrave: It is a fascinating decision, not yet translated to English, but there the Federal Constitutional Court has struck down as unconstitutional a piece of legislation in North Rhine-Westphalia which was enabling covert online reconnoitring of internet activity. So activity like the covert placement of Trojan horses on someone's computer system would be, as a point of departure, unconstitutional.

Q491 ***Lord Woolf:*** Did it do that because it was disproportionate or on what basis?
Dr Bygrave: It was on the basis that it conflicted with the right to informational self-determination, which is derived from two very broad provisions in the opening paragraphs of the German basic law and which give the court a great deal of opportunity to review surveillance measures on a case-by-case basis. In this case they have been claimed to have invented a new right now, a right to protection of personal computer systems, though on the basis of this right to informational self-determination.

Q492 ***Chairman:*** Professor Koops, would you like to comment?
Professor Koops: Yes. I agree with Dr Bygrave that a written constitution is only useful if you have a good constitutional review. You should have a constitution with teeth, because just having a right on paper is not sufficient. I should also add that, obviously, we have a European Convention on Human Rights and Fundamental Freedoms which is valid for all European countries, members of the Council of Europe, and, through the Human Rights Act, is also implemented and valid in the UK, although I am not familiar with the particulars of it. The problem with, for example, Article 8, the right to privacy, in the European Convention is that there are exceptions to this right, which, although formulated very strictly on paper, (privacy can only be limited if it is necessary in a democratic society), in practice can be interpreted freely by governments saying, "We just think that it is necessary because we have much more organised crime", without any empirical evidence of what the need is. It is more a matter of privacy being, as I said before, valued by practitioners, like High Court judges, and the source of privacy is not so much important. The example that Dr Bygrave gave is a good example of privacy being held up in Germany, not as much because it is in the constitution but because, for historical reasons, they really know the need, and other countries which have similar constitutions but do not hold privacy in such a high regard can much more easily interpret the words differently. So it is not really the lack of a political constitution in the UK that would be the most important factor of validity.

Q493 ***Lord Peston:*** I think my question is aimed mainly at Dr Bygrave but it may well be for our other witness as well. Until I sat on this committee and we did this inquiry, if you had said to me that you thought Germany was a freer society than our own, I would have said you are mad, and I think most people in this country would take that view; and if you were to suggest to me that the Swedes were a less free society than our own, with lots of Swedish friends, I again would have said you are mad. Is not the problem here possibly with the researchers looking into these matters rather than the reality, particularly the German case? I find it quite absurd that anybody would regard the existence of their constitution, or the example we were given, I think, last week that their railways could not issue a credit card because this might lead to the return of Heinrich Himmler. Again I would say, Germany had a terrible time and I understand why they have a got a constitution, but the notion that any of that is relevant to the problem of our society I find very puzzling, and I put it to you strongly that way so that you can respond, but what is your response?
Dr Bygrave: Certainly David Flaherty was accused by some people of being an outsider and not properly understanding the complexities of the jurisdictions he was looking at. Particularly Scandinavians reacted at his conclusion about Sweden and felt that he was being unjust, and that may be so. Nevertheless, I think it was a pretty honest attempt to make some sensible comparative considerations, and it was one that was done on the basis of extensive interviewing and empirical research. He was not cutting corners, but obviously he stepped on toes with his conclusions. To get back to the point I made earlier, in every day life I do not think the quality of one's daily routines is significantly different in the UK to Germany to Sweden to Norway to Portugal. I think most people experience that they have a reasonable amount of freedom. A lot of the debates at research and policy level are about certain legislative initiatives that seem to fly over the heads of most people and, indeed, often never hit them, so that gives some of the debate a somewhat abstract quality, but, nevertheless, they are very important debates.

Q494 ***Lord Rowlands:*** I wonder if I could perhaps, Professor Koops, return to the constitutional point. In your very interesting appendix to the evidence you gave us in paragraph 8.3.2., where you discussed very helpfully data protection, you then say that there are data protection principles: "Constitutionalization of these principles . . . is to be recommended." Can you elaborate on this aspect of constitutionalizing data protection principles?
Professor Koops: There are various ways in which you can approach data protection. We have a large body of data protection ground rules emanating from Convention 108 of the Council of Europe and with the European Directive outlining data protection principles. The fact that we said in our overview that data protection principles merit constitutionalization is that the instruments of data protection so far, the Data Protection Directive and the Data Protection Acts in most countries, are laws which can be interpreted broadly, and they are very complex and hard to implement laws and, because the instruments are so complex and hard to implement, hard to live

up to, so it would help if you have a few, a handful of clear principles that say this is why data protection is important. Data protection is important because, in my view, it is about fair treatment, equal treatment, being treated fairly in social life, and that means that there are a few basic ground rules that you should live up to. The data finalisation principle for example: you should have a purpose and you should stick to that purpose, and not use data for other purposes—one of the most important principles, I think—and should that be constitutionalised, although it is not necessary, it would be sufficient to engrain the need for such principles better in the minds of politicians and members of Parliament and governments.

Q495 ***Lord Rowlands:*** If you were doing that, how would you amend the UK Data Protection Act, by incorporating what, a series of principle statements? How would you do it?
Professor Koops: I do not think you can constitutionalize principles by amending the Data Protection Act, because the Data Protection Act is not part of the constitutional order.

Q496 ***Lord Rowlands:*** We have not got a constitution!
Professor Koops: I would not do that for this. I think in this case I would look, again, to the European Convention, Article 8. Data protection is part of that.

Q497 ***Lord Woolf:*** Do you not think that is a constitutionalized principle, Article 8 of the European Convention?
Professor Koops: Yes.

Q498 ***Lord Woolf:*** Does that not provide a constitutional base for judicial review in this country of data protection and data activities if the courts feel it is appropriate to do so?
Professor Koops: Yes, I think it does, but Article 8 of the European Convention is talking about data protection or is being interpreted as covering data protection in a very general way, it does not list the main principles, such as purpose specification and purpose limitation and audit and supervision. I think it could be sufficient, but it could help if the courts could also look at other instruments, like the Council of Europe Convention and like the European Charter of Human Rights, which, through the new European Order, will become part of the constitutional orders as well of all EU countries.

Q499 ***Lord Rowlands:*** Professor Koops, how robust are current conceptions of privacy and the concept of a reasonable expectation of privacy in the face of what in your evidence you called a cumulative move towards surveillance? Again I read your appendix with great interest that in various constitutions the idea of privacy is written in Germany into the concept of human dignity, in France it is liberty, in Canada and the US it is search and seizure of property, et cetera. How robust is the idea of a reasonable expectation of privacy currently embedded in liberal society's legislation and constitutions?
Professor Koops: I think you should make a distinction between privacy, and privacy as it is known and used in the constitutions and in the debates in Europe, for example the ones you mention, and the notion of reasonable expectation of privacy, which is a more Anglo Saxon and American conception of privacy. Privacy traditionally is seen more as a fundamental right; whereas in the United States it is being interpreted as developing over time, and as people face less privacy on the streets, because they get used to cameras, they have no reasonable expectation of privacy any more, so there might be a consequence of the use of the notion of reasonable expectation of privacy that you gradually diminish privacy because technology in society tends to develop in ways in which people get used to less and less actual privacy. Instead of trying to read the notion of reasonable expectation of privacy into the constitution, as you mention, it might be more worthwhile to look at the, as you mention, notions of autonomy and human dignity as the underlying values of privacy and to use privacy in such a way. I am not quite sure whether this answers your question.

Q500 ***Lord Rowlands:*** Dr Bygrave, do you have any comment on that at all?
Dr Bygrave: While the notion of reasonable expectation of privacy is a notion that has probably been furthest developed by the US Supreme Court under its Fourth Amendment case law, we do find it, nevertheless, creeping into European jurisprudence. The Strasbourg Court is increasingly using this notion to assess what amounts to an interference with respect to private life under Article 8, paragraph one. In a case involving the UK, for example, the *Halford* case from 1995, the court was able to say a person working in their office is entitled to a reasonable expectation of the privacy of their telephone calls; so any bugging of the telephone which is without consent and, indeed, without knowledge is going to be interference. Whether that is a good development or not can be debated, and I would agree with Professor Koops when he says that the problem is that you introduce a slippery slide that is not particularly effective in the face of growing technology applications and people's accustomisation to these. So, if you can say, like Scott McNealy did, "You have zero privacy. Get over it", obviously there is not going to be much purchase for any right to privacy based on a reasonable expectation of privacy.

Q501 ***Lord Rowlands:*** If there is a kind of cumulative move towards surveillance, as Professor Koops stated, how will the regulatory agencies keep abreast with it and, as it were, defend the citizen?
Dr Bygrave: It is difficult. They are in a vulnerable position, because on the one hand they are under a statutory duty to uphold privacy and privacy-related interests; on the other hand they cannot adopt policies that are too far out of step with public perceptions of what is reasonable. We had this situation come to a head in Norway recently over a debate about whether video surveillance should be permitted on public transport where the Data Inspectorate, which is the equivalent of the Information Commissioner here, went out very strongly against such surveillance, and yet there were public opinion polls indicating that most people wanted the video surveillance, they thought it was reasonable, and they seemed irritated over the more privacy-friendly approach taken by the inspectorate which was meant to be taken on their behalf. They did not want it; they wanted security.

Q502 ***Lord Peston:*** I am still worried a bit about the definition of privacy. Those of us who were brought up within the British education system and were taught essentially along the lines of what John Stuart Mill said thought there was an easily defined circle, at least Stuart Mill did, and that was the area of privacy, and his concept was that that was your business and no-one else's business. Am I not right that, largely for technological advanced reasons, you cannot draw that circle any more? Would you agree with that, that that is the problem, and that it has arisen, at least in part, from technology?
Dr Bygrave: Yes, partly technology, partly organisational or cultural practices in relation to technology. Technology never acts alone; there is always complex interaction between different factors. You see with the Strasbourg case law that you can have a right to respect for private life outside on a bridge going across a railway, so the public/private distinction is no longer as easily applied in the legal context as it was. Nevertheless, getting back to the Federal Constitutional Court in Germany, that has based a lot of its recent decision-making on this perhaps artificial notion that you do have an absolute private sphere into which the state cannot intrude, and that is particularly in relation to what happens in your own home, which is your castle, what you do in your own home with your friends, your family, in other relations of confidence, and that is a fairly definite border that the court has set up in an attempt to protect privacy interests against the ongoing development of technology and different organisational practices that would try to erase the public/private distinction.

Q503 ***Chairman:*** Professor Koops, would you like to add anything?
Professor Koops: Yes. I agree with what Dr Bygrave says. I should stress that I think it is no longer feasible to see this absolute sphere of privacy which is a close circle of privacy and to view that in spatial terms, because even in your own home you can nowadays be monitored, and you are being monitored. For example, thermal imaging, the heat that the house radiates can be monitored from the outside and increasingly cameras can look through walls, and you have body scans that can see through clothes. So, even if you feel you are in your private space you can still be watched, with or without your knowledge, and I think it is important that we find ways to transform this notion of an absolute circle of privacy in which you mind your own business and the rest have nothing to do with it, to view that circle not in physical terms but in terms of probably data, who has access to what types of data and which data are really your own, and not only terms of data but perhaps in more flexible terms of space. It is a bit vague, as I said, but I think we should try and find new notions of what exactly is your home where you can be yourself. What is your castle in a world where the home is no longer restricted by four walls?

Q504 ***Lord Morris of Aberavon:*** We have referred to the European Convention, Article 8 in particular. I want to ask with regard to the role of the courts in clarifying rights. Is not the Convention a very important trigger mechanism in clarification? How is jurisprudence being developed, is it consistent, and is it possible to have an objective quantification? Which of the liberal democracies has the highest degree of surveillance and compliance with the Convention?
Dr Bygrave: I will preface my remarks by saying that, generally, the courts have not had a significant role in interpreting and applying at least ordinary data protection legislation. In Australia, for example, there was not one court case of any significance on the Privacy Act, which is the equivalent legislation to the Data Protection Act here in the UK, for 15 odd years; a similar situation pertains in Norway and in Denmark; a similar situation also has pertained in the UK, although we do now have an increasing number of cases, the *Durant* decision, for example, probably being the most significant in recent years, a decision of the Court of Appeal, Civil Division. So courts have not had a significant role in clarifying the law in this area. Who has had that role? It has been primarily the data protection authorities through administrative decision-making, which has been somewhat problematic, I think, because in the first place a lot of that administrative decision-making has been poorly reported and, secondly, there has been perhaps a little bit of bias in the way in which those authorities interpret their respective pieces of legislation, which

is inevitable, because they are there to uphold privacy interests, so they are going to interpret their legislation in a privacy-friendly way, but when the courts have come in, they have come in often as a corrective, and a welcome corrective, I must say. They have stirred up the cosy club of data protection authorities and said, "Hey, no, you cannot necessarily interpret this particular provision in this way. In fact this is the better interpretation." One problem, though, is that the courts have not always developed a consistent line themselves. Look at the notion of personal data, which is a key notion for application of the Data Protection Act here and equivalent legislation elsewhere in Europe. We have, on the one hand, the *Durant* decision from the Court of Appeal, saying that personal data, as a concept, should be read down to only embrace data that implicates, as it were, the privacy of the person to whom it relates. On the other hand, we have courts elsewhere saying, at least indirectly, "No, that is not the case." There are some interesting decisions over the status of IP address data. For instance the Paris Court of Appeal has held, "No, IP address data is not personal data", whereas the Stockholm Administrative Court has held, "Yes, it is", with the Data Protection Commissioners in the form of the Article 29 Working Party agreeing with the latter. So there is great uncertainty over how to interpret a key notion in data protection law. Fortunately, we have Strasbourg, which is increasingly laying down a set of basic principles that apply to the data protection field, and those principles are now being applied by the European Court of Justice when interpreting the Data Protection Directive. The *Rechnungshof* decision is the leading case there, a decision of the European Court of Justice from 2003, saying you cannot interpret the Data Protection Directive without looking at the Article 8 European Convention on Human Rights case law. So Strasbourg increasingly is the baseline, at least here in Europe, but Strasbourg case law in itself is not always consistent and there are gaps and in some cases the case law has not come as far as the data protection legislation existing at national level. The right of access, for example, pursuant to Article 8 of the European Convention on Human Rights is much more restricted than it is ordinarily under data protection law at national level. That is quite a long answer. Maybe Professor Koops wants to supplement that.

Q505 ***Chairman:*** Professor Koops, do you want to add anything?

Professor Koops: Dr Bygrave has talked largely about data protection. We should stress, of course, that Article 8 also covers privacy of home and family life and correspondence and there, like with data protection, the European Court of Human Rights increasingly has many directional verdicts which are used by all the national courts, but, again, there are gaps there. How important is the jurisprudence for the overall protection of privacy? It is important, obviously, because it adds directional value, it guides the way that you should interpret privacy rights, but I fear surveillance is moving towards a paradigm of preventative measures in which you monitor large groups. This has effects on privacy, which diminishes the privacy of ordinary citizens, but that type of monitoring and surveillance rarely gets to the courts because it is preventative, and it might only get to the courts when people complain or when an odd thing happens, but the overall diminishment of privacy is just something that happens that is not brought in any case.

Q506 ***Lord Peston:*** Obviously you have been dealing with this in this way because Lord Woolf asked you a question about the courts, but speaking as a democrat, albeit a member of a totally non-democratic House, surely the real place for debating, guaranteeing is too strong, but at least clarifying concepts like privacy must be the parliaments rather than the courts. I am rather troubled. Courts have to interpret what parliaments have put forward, but in the end parliaments are what matter, it seems to me. Do you agree with that?

Dr Bygrave: Yes, I certainly agree with that. The general problem with the courts is, obviously, the democratic deficit which in theory you do not have with parliaments. The problem, nevertheless, is that parliaments in the present climate, with a war on terror going on that seems to have no end, are not necessarily acting as a sufficient corrective to the push for more and more security, and that corrective is coming both from the Data Protection Commissioners and from the courts. I would love to see the parliaments being a corrective in this area, but at least in some jurisdictions they are not. Rather you have political parties outbidding each other to be strong on the war on terror.

Q507 ***Chairman:*** Professor Koops, would you like add to that?

Professor Koops: Yes, I think that we need the courts to steer, to control, to supervise what the parliamentary legislature is doing, because there is such a wide scope of interpretation for the privacy rights. As Dr Bygrave was saying, in the current climate it is easy to say, well, in this case the privacy, although important, should weigh less than a security measure. I think there are two particular points of contention for parliaments which make it difficult to really hold up privacy. One is that—and this may be different in the UK but at least in the Netherlands and I think in quite a few other parliaments they are incident driven. They are talking about what is

important now and so they are talking about a single measure which seems important because with this you can prevent what happened last week, and so they look at each single measure, at each individual measure and, thus, do not have the overall picture and disregard the cumulative effect which all these measures together have on privacy. The second point of contention is that we are often talking about complex measures, computer technologies, and the precise functioning and what the technologies can do requires some knowledge of technology, which again in the UK, members of Parliament may be an exception, but many do not know much about what technology does, so they have people imagining what the precise effects will be of implementing these technological methods, which is particularly important when building infrastructures with large-scale technology that is put in in society, such as surveillance cameras, biometric passports, which once there are hard to reverse.

Q508 ***Lord Smith of Clifton:*** It is very interesting. You have talked about the courts and the regulatory agencies and the parliaments but you made no mention of those vital parts of civil society which are the informal pressure groups, and they make up the democratic deficit to a great extent as guardians of civil liberty. Have there been any studies of the role of pressure groups across the EU Member States with particular interest in protecting civil liberties?
Dr Bygrave: I am not aware of any systematic study. I would suggest Professor Raab may be better placed to answer that question than myself, but you have made a very important point. Those sorts of pressure groups tend to be most prominent and vocal in the USA, where we have, for example, the Electronic Privacy Information Centre and the American Civil Liberties Union. These are actors that have an important role to play, although the degree to which their efforts ever result in concrete legislative action or concrete legal policy is debatable, but they are important in igniting public debate. I notice in Scandinavia those sorts of organisations do not have the same sort of role. People trust government to do that sort of thinking for them—misplaced trust in my opinion.

Q509 ***Lord Smith of Clifton:*** Hear hear!
Dr Bygrave: Here in the UK one has Privacy International, but that is effectively a three or four person operation.

Q510 ***Lord Smith of Clifton:*** There is No2ID and there is Liberty, of course.
Dr Bygrave: Yes, Liberty has played an important role in many policy areas.

Q511 ***Chairman:*** Professor Koops, would you like to add anything?
Professor Koops: I agree that pressure groups are very important because they can play a role in debates by giving information, by highlighting possible effects that in the general debates tend to be overlooked, but, as Dr Bygrave mentioned, internationally they are usually quite small, with a few people, often volunteers, with limited resources, and so there are only a limited amount of topics that they can monitor. More importantly, if the question is: do they not fill up the democratic deficit to a large extent? No, they never can, because they have no power. Their function is to highlight evidence, to signal, to give information, but they have no influence directly, they very indirectly have influence, but they have no power to say this measure should be not adopted, like parliaments, like the courts and data protection commissioners have, so they could never fill up the democratic deficit.

Q512 ***Baroness O'Cathain:*** How important is it to have a well resourced and independent regulatory authority for enforcing data protection, privacy and for keeping surveillance under control, and is it actually feasible to have one regulatory authority making sure that all three are treated equally?
Dr Bygrave: I think it is important to have a well resourced and independent regulatory authority. There is no question: such authorities do make a difference. I can point to many concrete examples where authorities, such as the Information Commissioner and his staff, or her staff, as it used to be, have come in and made a difference to concrete policy being rolled out. In Norway there are numerous instances where the Data Protection Authority has put a stop to fairly controversial plans for data-matching, not just within the public sector but also the private sector, and they have been able to do so under a scheme which, basically, meant that lots of these controversial projects had to be approved by the authority in the first place. That sort of scheme is not always easy to put in practice because it is very bureaucratic and it is demanding of resources and these authorities are not usually well resourced. That is the big problem: they are not well resourced. Getting back to our friend David Flaherty, who I mentioned earlier, he came with a comment in his study which questioned whether such authorities were always a good idea. He said such authorities may, in fact, add legitimacy to surveillance measures, if they function effectively as a rubber stamp approval process where they can say, "We approve this process", but they have not had the resources or the guts to go in and make a very good and sound assessment. But that is also a criticism you

could mount against data protection law and other pieces of law that are ostensibly upholding privacy interests and giving citizens the feeling that, yes, privacy is being cared about but really do not have much bite. As I said, there are nonetheless numerous instances where data protection authorities have made a difference. An interesting point also, I would say, is that you just do not need a well resourced and independent regulatory authority, but you also need one with effective powers of intervention. Those effective powers of intervention do not necessarily have to flow from a scheme where you get prior authorisation from such an authority before you can proceed with data-matching or data surveillance practice. Flaherty's study showed that, indeed, the German data protection authorities, which really are only ombudsmen, in the Scandinavian sense at least—they can only make recommendations—nevertheless, because of the particular personalities of these officers, their persuasive powers, their networks, were able to stop or at least dampen some of the surveillance efforts. Two other points. One is that you cannot rely solely on the courts. Court litigation to uphold your rights is, for most people, just too expensive and it is too time-consuming, so you need another avenue, you need another friend, as it were, to bring your complaints to, and data protection authorities are very well placed to be that type of body. You need also a voice in international fora to thrash out privacy policy; and more importantly you need a body that plays an educational role. In other words, I would say you do not just need a well resourced, independent regulatory authority with effective powers of intervention, but you also need an actor that has an educational role and undertakes that role seriously. A problem so far is that these authorities usually have not had the resources to undertake significant educational efforts. There have been some good initiatives. The 'Protecting the Plumstones' CD-ROM that the Information Commissioner was responsible for producing and sending to schools here in the UK is a very good example of educating young people about civil liberties, about privacy problems with respect to ICT, et cetera, but we need more of those. Finally, legally it is a requirement to have at least an independent regulatory authority. The Data Protection Directive specifies this in Article 28. And if you look at the provisions encapsulating the new right of data protection that Professor Koops referred to earlier, you will see that the third paragraph of those provisions states, in effect, "Compliance with data protection rules shall be subject to control by an independent authority." This is in Article 8 of the Charter of Fundamental Rights from 2000 and in Article II-68 of the European Constitution from 2004, which will probably never enter into force.

Q513 ***Chairman:*** Professor Koops, would you like to add anything?

Professor Koops: I would like to stress the point that Dr Bygrave made that regulatory authorities should not only be well resourced and independent, those are two fundamental points, but should particularly have strong teeth and sanctioning powers. I would add that I see two functions for regulatory authorities: one is to supervise the way that data protection law and also privacy law is being implemented and lived up to in practice—that is one type of activity—but I think the other role could be equally important, and should be equally important, which is to provide parliaments with advice on intended legislation, which is the role that at least the Dutch Data Protection Authority has and, I presume, many other data protection authorities as well. The problem is that they have no sanctioning powers about their advice and often what you see is that the Government says, "Yes, we have read the advice. It is all very nice, but we think differently, and so we just go on with this surveillance measure". If Parliament does not then stand up and say, "We take the advice of the data protection authorities seriously", there is no real effect on privacy and protection data, and so in some way advice from such a regulatory authority, if it is within the legislative process, should have a real value and weight, otherwise it is not much use.

Q514 ***Baroness O'Cathain:*** You say that the regulatory authorities should supervise the information being implemented and advise Parliament and do a bit of pre-legislative scrutiny, but surely is there a third role which would be to be independent and start an investigation of their own if they feel there is something going wrong?

Professor Koops: Yes, but I think that is part of the first role in supervising the implementation. They can do that in two ways: one by a complaints process, and so it is a reactive role, but there is a proactive role, "This branch might be a bit fishy, let us look into it." We should also have an authority that looks at: does not the state do things which warrant looking into echelon-type of researches? I think that would be a good role, but it is not necessarily the regulatory authority, data protection authority that should do that.

Q515 ***Baroness O'Cathain:*** I really had one idea, and that was if something was being done, say, in the states or in one of the countries in Europe which had not actually spread over to the other 26 European Union countries, the regulatory authority in country A could say to the Government, "Really we ought to look at this. We want to look at this", and then recommend. That is a proactive, which I think is not

quite covered in what you said about supervising information being implemented.

Professor Koops: That would be a very useful function. It is not necessary to have the supervisory authority in that role. It might also be members of Parliament who trigger such things. For example, in European parliaments you often see that it happens in that way.

Q516 ***Chairman:*** Professor Koops, can I thank you on behalf of the Committee for your virtual presence with us and the evidence which you have given, and Dr Bygrave for coming all the way from Norway to be with us and for your evidence. I hope that the rest of your stay in London is enjoyable. Thank you very much indeed.

Dr Bygrave: Thank you, my Lord Chairman.

WEDNESDAY 2 APRIL 2008

Present	Bledisloe, V	Quin, B
	Goodlad, L (Chairman)	Rodgers of Quarry Bank, L
	Norton of Louth, L	Rowlands, L
	O'Cathain, B	Smith of Clifton, L
	Peston, L	Woolf, L

Examination of Witness

Witness: PROFESSOR DAVID FELDMAN, Rouse Ball Professor of English Law, University of Cambridge, examined.

Q517 ***Chairman:*** Professor Feldman, good morning. Thank you very much indeed for coming to join us. It is extremely good of you to give your time. We are not being televised this morning, but we are being recorded, so may I ask you, please, to formally identify yourself for the record and then, if you would like to make a brief opening statement before we start questions and discussion, that would be most welcome.

Professor Feldman: I am David Feldman, I am a Professor in Cambridge and Chairman of the Faculty of Law at the University of Cambridge, a Fellow of Downing College and a judge of the Constitutional Court of Bosnia and Herzegovina. I am very grateful to your Lordships for inviting me to come and contribute to the inquiry. All that I think I would say to start with is that I am not entirely convinced that surveillance generally raises important constitutional issues of an institutional kind, but I think that it affects a number of the underlying values that help to support the constitution, and perhaps it is those matters that we will be concentrating on mainly. Apart from that, I am here to answer questions.

Q518 ***Chairman:*** That is very kind. Thank you very much indeed. Perhaps I could kick off by asking if there are, in your view, any existing constitutional conventions or principles that are threatened by the spread of surveillance and data collection and are there principled limits that we, Parliament, might want to impose on the state's powers in this area?

Professor Feldman: I do not think that there are any constitutional conventions that are particularly affected. The one that might be perhaps is accountability, if one regards accountability for surveillance activity as a constitutional convention. I am not sure that it is actually. It may be that one particular form of it, ministerial responsibility to Parliament, is a clear constitutional convention that is engaged where the activities are undertaken by or under the control of a minister. I think it is extremely difficult to see how that convention can operate in relation to activities of other agencies and still more difficult to see how it can operate where the activities are undertaken by private organisations. Of course, a lot of surveillance, for example, by CCTV is undertaken by private people, private bodies, and that lies outside the convention of political accountability entirely. On the other hand, constitutional principles, as I hinted a minute ago, are significant and I think that there are two or three that might be relevant. First of all, as a general background principle supporting the idea of liberty in this country, the UK's constitution has long relied on what one might describe as a principle of executive and legislative self-restraint in interfering with people or authorising interference with people and their activities. That is an important principle, although it is very rarely written about in any of the text books, and it is important because of the centrality of the idea of the legislative supremacy of the Queen in Parliament. If you have a situation in which the Queen in Parliament can authorise in principle anything, then it becomes very important to be self-controlled in the way in which those powers are used, so I like to think that there is a principle of both executive and legislative self-restraint that is increasingly under strain, I think, at the moment. In relation to the executive, that was made more pressing by a decision of Vice-Chancellor Megarry in the late seventies in the case of *Malone v Metropolitan Police Commissioner* where he extended the view that people could do anything that was not forbidden by statute or common law to the police and, by implication, other state agencies.

Q519 ***Chairman:*** Can you remind us what the point at issue was in the *Malone* case?

Professor Feldman: The *Malone* case concerned telephone tapping, allegedly by the Metropolitan Police. Mr Malone, who was the subject of the alleged interception, sued for a number of grounds, all of which failed, and they failed because there was at the time no legal rule preventing anyone from tapping anyone else's telephone and Vice-Chancellor Megarry said, "This is a free country. Because it is a free country, you can do anything that is not forbidden, and that applies to the police as it applies

to you and me." That is a problem if you believe in the Rule of Law as a system for imposing legal accountability and objectively verifiable standards on activities by public and executive bodies that interfere with people's private activities. So it was objectionable as an attack on the spirit of the Rule of Law. It also ran counter to other decisions going back a very long way, at least into the 18th century, holding that actually the Executive needs to show positive legal authority for what it does if it affects people's rights. That was one reason why it was problematic. Another reason was that, as Vice-Chancellor Megarry foresaw, it meant as a state we were acting inconsistently with the rights with respect to private life under Article 8 of the European Convention, and I think, probably, there is a constitutional principle that, as far as possible, one ought to make sure that one's executive, legislative and general legal arrangements in the state are consistent with our international obligations.

Q520 ***Chairman:*** Do you think that the constraints under Article 8 on proportionality and, indeed, necessity are adequate?
Professor Feldman: I think the answer to that is that it depends, my Lords. Article 8 imposes what are essentially the requirements for justification of interference with respect to private life, family life, the home and correspondence broadly defined, very broadly defined. It requires, first, that there should be a legal basis for the interference in positive law, as much as Article 8, paragraph 2(b) says in accordance with the law, and that means it must comply with the requirements for provision of positive law regulating and authorising the activity. That was held by the European Court of Human Rights to be lacking in the *Malone* case when the *Malone* case reached Strasbourg. Then it requires that the interfering authority must show that the interference serves a legitimate aim, and that is not too difficult a job to meet. Lastly, as you say, it requires it to be shown to be necessary in a democratic society, which includes a proportionality requirement. That can be a substantial burden on a justifying agency, but whether it is a really robust protection depends on how effectively the reviewing body applies the proportionality test and also how carefully the body which has to authorise the interference in the first place applies it. If it works well, it can be a very effective protection indeed, and my impression, for example, is that the Information Commissioner and the Information Tribunal under the Data Protection Act 1998 make very good use of proportionality tests and are very effective. If one were to adopt, as some people say that courts ought sometimes to adopt, a more deferential view to the question of proportionality and treat with considerable respect the view of the original decision-maker as to whether the interference was justified and proportionate, that would be a much less useful protection.

Q521 ***Baroness Quin:*** I wanted to follow up something you said in your first reply when you talked about the Queen in Parliament being able to press anything and, therefore, a kind of self-regulation being appropriate. I do not know whether I picked it up right, but was there a concern that self-regulation is perhaps less effective than it was and, if that is true, what is the cause of it? Is it media pressure, or events to deal with terrorism, or what?
Professor Feldman: I think it is considerably less effective than it used to be, and the best evidence for that is to be found in the number of powers which have been granted by Parliament for surveillance activities and for exchange of personal data between agencies with remarkably little in the way of substantive criteria attached for deciding when such exchange should be permitted and how the regulatory scheme should be given effect, where there is a regulatory scheme. To some extent that was undoubtedly the result of concerns about terrorism, but I do not think it is only terrorism. It was happening way back in the eighties and nineties. We had Northern Ireland related terrorism, but it was before what we now think of as international terrorism became a major concern, and it is a combination of security concerns with concerns about certain types of crime, particularly financial crime, serious fraud, tax and social security crime and, more generally, a desire to ensure that people are providing information that the state needs, or thinks it needs, for whatever purposes seem good to the agency, rather than starting from the proposition that people are entitled to keep their business to themselves and that very special and immediate justification is needed to interfere. In a sense (and this may be over dramatising it slightly) one might say that we have moved from the position that we were in when I was a student of law some 35 or more years ago where we were told that, as a matter of constitutional law, we were all subjects of the Crown, not citizens of the state, and yet we were left to a very large extent on our own and not interfered with, to a point where we are now told the whole time that we are citizens, and yet the implication of that seems to focus on our responsibilities to the state and we are treated, as it were, as a resource for the state and as a source of useful information and even in some cases—for example, the plans for the identity card—we are made to pay for the privilege, and that seems to me to be somewhat paradoxical. It is a change of attitude on the part of our rulers to us which is, I think, a reflection of a sea change in the nature of our relationship with the state.
Chairman: Thank you very much.

Q522 ***Viscount Bledisloe:*** I have two questions about *Malone*. First of all, has it been judicially or text-bookly commented on and, if so, favourably or unfavourably, and, secondly, I fully understand that individuals are allowed to do anything they are not forbidden to do, but I thought that state authorities, and so on, were only allowed to do what they are authorised to do by statute and if they could not find the express power to do it they could not do it?
Professor Feldman: Yes. To take the first point, there have been unfavourable comments on the general approach adopted by Vice-Chancellor Megarry, to be found in quite a large body of literature, and, of course, it was a view that Vice-Chancellor Megarry himself adopted with a certain amount of reluctance because he foresaw that it was going to run straight into the Rule of Law type of requirements of the European Convention, but there is no shortage of critical literature. The general approach, however, has not changed particularly, and the reason for that is that the Vice-Chancellor was hampered by the fact that in this country, at least until the passage of the Human Rights Act 1998, there was no source of what one might describe as a right to privacy in the law of any of the jurisdictions of the United Kingdom. So, the question that he asked himself was, "Have the police done anything unlawful by interfering with the telephone messages and communications of the plaintiff?", and the answer was, "No", because it involved no trespass to property, in the circumstances no breach of confidence, and there was also no right to privacy that could stand on its own. So he said there was nothing unlawful about what they were doing: there is no positive authority for them to do it, but they do not need that because the constable is just a citizen in uniform, or a subject in uniform. That was the basis of the *Malone* case.

Q523 ***Viscount Bledisloe:*** It was treated as the act of an individual rather than as the act of a statutory authority?
Professor Feldman: Yes. It would be true also, I think, of a secretary of state or anyone else operating in a dual capacity. My Lord Chairman, there was a second question which I do not know whether Viscount Bledisloe might like me to answer. I cannot remember what it was though!

Q524 ***Viscount Bledisloe:*** I think you almost answered it. My question was: is there not a difference when this is a body set up by statute or by the state as opposed to an individual?
Professor Feldman: Yes, it is true that if it is established by statute and it has only statutory powers, then those probably are the only statutory powers that it has, although there is a view that even statutory bodies can exercise certain common law freedoms. For example, most statutory bodies can hold property and in relation to their property holding they exercise ordinary property rights, subject to perhaps the opportunity to conduct judicial review, on public law principles, of the use that is made of the property. But in principle I think I think there a distinction between purely statutory bodies and others.

Q525 ***Lord Rowlands:*** In some of the written evidence we have received one our witnesses makes a very powerful point that there is no over-arching principle, it is built up piece-meal. I think at the beginning of your answer you started identifying possibly one of these principles, the issue of liberty. What about the right to know? The citizen has a right to know what information is being held by agencies. How far is that currently enshrined?
Professor Feldman: It is quite extensively enshrined in our law in a number of different forms and from a number of different sources. Most obviously, there is the Data Protection Act 1998, and in principle that covers all personal information held by anyone in a form which allows it to be processed so as to identify individuals and applies to all personal information, and there is a heightened regime in respect of certain types of information the Act calls "sensitive personal information". The impetus for that came from a number of sources, both concern about control of sensitive information within the UK and also a European Community Data Protection Directive—I think it was 95/46—and the 1998 Act was enacted as a response to our obligations under the Data Protection Directive. The Data Protection Directive itself refers to, and is a practical manifestation of, the principles set out in the European Convention on Human Rights, particularly Article 8 (the right to respect for private life, and so on) that we have already discussed, and Article 8 of the Convention, as interpreted by the European Court of Human Rights, has now for a long time included quite extensive requirements for states to take action to control the use that can be made of personal information. The way in which these principles work is that there are several different points in the information gathering and use cycle at which obligations to the data subject (as the person who is the subject of the information is called) can arise. First of all, at the point of gathering the information, the Data Protection Act does not, on the whole, say much about gathering.

Q526 ***Lord Rowlands:*** So you can gather it without permission, without consent?
Professor Feldman: Yes. The Data Protection Act kicks in particularly once people hold personal data, because it controls obligations in relation to the security of storage of data, the period for which it can be held, the purposes for which it can be processed

and the ways in which it can be processed, the circumstances in which it can be disclosed to others and the rights of the data subject in relation to the information, and they include, generally speaking, rights, for example, to find out what information is held by a particular agency, a right to ensure that it is accurate, a right to ensure that it is only processed for the legitimate purposes for which it is being held and that disclosure meets the sort of criteria that are set out in Article 8 of the European Convention, and there is a regulatory regime which is pretty effective, on the whole, at coping with that. The difficulty with it is that there are limitations on the circumstances and the extent of the obligations to the data subject where information is held—for example, for crime prevention and crime detection purposes—and right the way through the provisions there are exceptions that say that certain of the rights of the data subject and the data protection principles do not apply or do not apply with their full force if the applying of them would seriously prejudice the ability of the agency to do its proper job.

Q527 ***Baroness O'Cathain:*** Professor Feldman, you gave all those instances about the rights to whom the information can be disclosed. Is there any right for people to sell the data? For example, an enormous number of marketing groups actually go and buy data from state agencies as well as from everywhere else, and I do not think that the ordinary man or woman in the street has really got any idea of the extent of this, but is that covered by these rights that they can actually sell it, a state agency can sell the data that they hold on individuals for a considerable price, if they want to?
Professor Feldman: In principle the general answer is that there is no right to sell data unless the data subject has agreed to that use of the data. It is hard to imagine a situation in which the sale of data could fall within one of the legitimate justifying purposes under either the Data Protection Act or the European Convention, Article 8. There are, however, a number of isolated statutory situations in which the sale of data may be authorised. For example, I think, although I do not have this at my fingertips, there was a statutory provision that allowed doctors to sell certain medical data to drug companies for research purposes, but that is always an exception to the general principle.

Q528 ***Baroness O'Cathain:*** Can I pursue that point? People are still not aware that it is being sold. For example, if you subscribe to a magazine like Vogue, et cetera, there is always on the bottom of it a little box that says, "Are you agreeable that your details can be sent or given to other people?" They never say, "Can be sold to other people". I am wondering, is there any way of stopping this, because, in fact, at the other end of the process there is an enormous amount of junk mail which goes through every letterbox in the country of anybody who subscribes to anything or is on the data register, which is just so infuriating, and it is all being sold. Is there anything to stop it?
Professor Feldman: If the information that is held is personal information, then I see no reason why a complaint to the Information Commissioner would not have a good chance of success. If it is not personal information, then the—

Q529 ***Baroness O'Cathain:*** Are names and addresses personal information?
Professor Feldman: Addresses would be, yes.

Q530 ***Baroness O'Cathain:*** It is widespread, I can assure you.
Professor Feldman: Residential addresses.

Q531 ***Lord Peston:*** In fact, you have answered virtually all of my questions apropos of the Chairman's question, but there are two concepts or words that keep appearing here. One is the word "creeping"—creeping when it comes to surveillance. In other words, it is not happening as a planned change in our society, this creeping, it is your view that what we are observing here is a sort of creeping increase in these things. The second question, which may be less for a lawyer and more for a sociologist, is: is this creeping phenomenon inevitable or not?
Professor Feldman: There is certainly creep, yes, and it may well be inevitable because one of the features of legislation that confers new powers on any agency is that they start by conferring it to deal with what is billed as an exceptional problem or threat, and usually the power is nicely limited and it is subject to carefully thought out safeguards which provide a graduated system for ensuring that the use of the power is properly limited and proportionate. It then becomes, as it were, normalised and increasingly drifts across into other functions, other agencies, and at the same time what tends to happen is that the safeguards, which were carefully thought out at the initial stage, get watered down, and that is a pattern which has been a common feature of police powers, data sharing powers, a whole range of powers to obtain and then use information across a very wide range of statutory fields. If that is a sociological observation, then I suspect that it is inevitable.

Q532 ***Lord Peston:*** The example I was going to use, but in fact it slightly anticipates question three, is Terminal 5, where they were going to use fingerprinting—I think it was for 48 hours per person—simply as a way, as it were, of protecting various things inside the terminal. That seems to me an example of creep in the most forthright terms. It would never have occurred to someone a few years

ago, surely, that an organisation, in this case a private one, would use fingerprinting as a method of dealing with passengers.
Chairman: This is the British Airports Authority?
Lord Peston: The British Airports Authority.
Chairman: New Spanish practice!

Q533 ***Lord Peston:*** Or whatever it is. The Spanish practice is actually for methods of stopping things happening, particularly employment for non-union workers! Is that not a good example of what would have been regarded as simply laughable even ten years ago, that an organisation would think that? There was a fuss, and so it got dropped, but the fact is that they thought that that was a perfectly reasonable thing to do.
Professor Feldman: Indeed. One of the interesting things about the fuss was that it was led by the Information Commissioner, and it was led by the Information Commissioner because although the British Airports Authority is a private organisation, it is subject to the Data Protection Act, so it falls within the jurisdiction of the Information Commissioner and the Information Tribunal and it is a good example, I think, of how the protections offered by the Data Protection Act can be effective both at the planning stage, the pre-implementation stage, and at the subsequent stage. The position is rather different if one looks not at the data protection aspect directly but at, for example, CCTV surveillance: because there we are in a situation where for the last ten or 15 years the number of cameras in public and private spaces has grown exponentially; at the same time there is no regulatory regime at all. The security industry has a rather weak self-regulatory code of practice, individual local authorities have their own codes of practice, but the only thing that we have in legislation is a blanket authorisation for local authorities to set up cameras in public places for the purpose of crime protection and prevention. There nothing restrains it, and if one looks, for example, at the Home Office website, where one might expect to find the Executive would begin to support the regulatory process in some way by laying down standards, more or less all you find, or all I found a couple of days ago when I had a look, is a very large number of circulars and notes of guidance for people as to how to make their CCTV coverage most effective from a technological point of view, and that, I think, is a sign of failure of responsibility.

Q534 ***Chairman:*** Can I ask as a supplementary, before moving on to Lady O'Cathain, Professor Feldman, if you think that surveillance or data collection represents a threat to constitutionally established understandings of citizenship in this country and if the Human Rights Act and the Data Protection Act provide adequate protection for privacy or if there is a need for additional constitutional protection of citizens in connection with surveillance and personal data and, if you think there is such a need, what form might it take?
Professor Feldman: My Lord Chairman, as far as the constitutional understanding of citizenship is concerned, we discussed a few minutes ago how the changing idea of citizenship had been moved from subject to citizen and how it had not actually, in my view, been reflected in any valuable enhancements in the freedom or rights of the newly defined citizens; so I do not know that there is a constitutionally established understanding of citizenship in the UK and, that being so, it is hard to know how these technologies might affect it or change it. I do think that there is an effect on the relationship between various arms of the states. If I can enlarge on that a little bit, the process that I have already mentioned, whereby powers are conferred on administrative agencies with very wide discretion, with very little in the way of controlling or constraining principles, does provide a shift of power between the central executive and Parliament and agencies out in the fields doing things with information and obtaining information, a distinct shift of power, new power, to those agencies in the field. I also think that we have a responsibility as a state, the legislature has a responsibility, to make sure that a coherent look is taken at the grounds on which these activities could be undertaken, the people by whom they could be undertaken and the purposes for which they could be undertaken and then the use that could be made of the information afterwards. There is a patchwork of pieces of legislation, some of which are actually very good at setting standards and criteria. For example, I think the Regulation of Investigatory Powers Act 2000 did a good job on the powers that it covers for the agencies that it covers; I think the Data Protection Act 1998 did a good job as well on the data protection side of things. There is nothing on the sort of issues relating to control of surveillance in public space by camera and film. There is a certain amount of academic literature on the effects of that, but there is no legislative attempt to oversee that, and that is unfortunate. I do not know whether I have answered your question.
Chairman: Indeed you have. Thank you very much.

Q535 ***Baroness O'Cathain:*** Is there something inherent in this exercise of surveillance power that means that it is a threat to the rule of law and the notion of accountable constitutional democracy? Are there state employees who, in order to protect the Rule of Law, should be particularly subject to restrictions on their surveillance activities?
Professor Feldman: The answer to the second part of the question, I think, is yes, but then I think the answer to the second part of the question has to go on

to say it already is to a large extent regulated. Where state employees are doing it, it is regulated by the piece of legislation that I have just mentioned, plus the Human Rights Act 1998, and the case law from the European Court of Human Rights became relevant as a result of that Act. The answer to the first part of the question is that I personally do not think that there is anything inherent in the nature of surveillance and data collection that raises problems of that kind; it all depends on the form of the legislative scheme, if any, that is put in place to regulate it and the methods of accountability that are put in place. If you have surveillance introduced without any form of regulation or accountability other than legal law or effectively political, then there is a serious problem, but that is contingent on the way in which the legislature allows schemes to be introduced rather than being inherent in the schemes themselves.

Q536 ***Baroness O'Cathain:*** Can I give a hypothetical example? Say, for instance, there was a gang of 20 or so youths in a shopping precinct on a Friday night, having had far too much to drink probably, and they suddenly come across the surveillance cameras and they decide that they just do not like this and they do not see why they should be the subject of surveillance, no matter what they were doing, and even if they were not drunk, and if they decided to knock out these cameras they would be breaking the law, obviously, would there be any excuse for them so doing? Surveillance can actually be quite threatening, irritating and infuriating.
Professor Feldman: They can, and there have been studies of that sort of thing. The Home Office itself has done a study on the effects of CCTV surveillance, and there have been a number of sociological and psychological studies, including one or two by my colleague in Cambridge, Professor von Hirsch, looking at what sort of interests, psychological interests, are affected by surveillance and how. There are some consistent themes in the admittedly rather sparse literature. One is that CCTV surveillance can be very beneficial in at least discouraging or perhaps displacing certain kinds of offence and to that extent can be very reassuring to some people who find it helpful to have what feels like a more secure or less insecure environment. On the other hand, there is a compromise involved, a cost involved, in that, and that is that we may reduce our capacity to be ourselves in public spaces, and by "public spaces" I mean what are actually technically private spaces like shopping arcades as well. It is easy to see how one might feel intimidated, for example, if one were a gay couple holding hands in a public place if one thought it might get back to one's employer. One can see how it might look intimidating if one wanted to behave in a way that is perfectly lawful but a little bit abnormal; it leaves no space for withdrawal when one is in public; it leaves no space for collecting one's thoughts and moving on. That is a loss, which can be a significant loss, and it is hard to quantify the importance of the loss, but it is a fact, I think, that in Cambridge, for example, it is more or less impossible to walk 100 yards without being captured on at least one security camera. That I find slightly worrying.

Q537 ***Baroness O'Cathain:*** But then again, if somebody just gets really furious about that, they might just be walking along the street in Cambridge and just say, "I have had enough of this", and get a brick and throw it at it.
Professor Feldman: Yes.

Q538 ***Baroness O'Cathain:*** That could be constituted as actually encouraging problems.
Professor Feldman: May I suggest a number of matters that might need to be thought about if one were trying to decide whether that would be justifiable. First of all, it would be more justifiable to do that, I suggest, if one discovered that one was being covertly surveyed than if one knew that surveillance was taking place. Secondly, it might be more justifiable to take direct action against the surveillance if one knew or suspected that there was no effective regulation in place, apart from your direct action, to control the places where the surveillance was taking place, the circumstances where it was taking place and, perhaps most importantly, the use that could be made of the tapes. Thirdly, it may be that one would feel more justified in taking direct action if the nature of the surveillance were more rather than less intimate. For example, one could have different kinds of camera surveillance. One could have a generalised sweep with no focusing possibility—that is a relatively low level of intrusion; one could have focusing and zoom capacity, which would allow the operator of the camera to target particular people without letting them perhaps know that they were being targeted—that is more intrusive and might, justifiably, elicit a more aggressive response; and then if one knew or discovered that there was an audio capacity as well (there is in some of these cameras, although a lot of local authorities have accepted in their codes of practice that they will not make use of audio capacity), that would be a very serious interference with one's intimacy and ability to carry on ordinary, private conversations and activities and would be much more difficult to justify and so perhaps might make it easier to justify direct action. I am not exhorting anyone to go and take a brick and smash your nearest camera, but those are the sorts of nuanced considerations that too often get ignored when one tries to think about things in very broad terms. The reason, I think, that it is ignored, although I should say not by Professor von Hirsch, on whom I

have drawn for some of those distinctions, is that there is no legislative scheme. The legislature has never turned its mind to these issues.
Chairman: Until today.

Q539 ***Lord Woolf:*** I wonder if I may ask a question following up from your answer. Professor Feldman, I apologise that I was late. Is there any concept of self-help in relation to breaches of the Human Rights Act? Has that ever been considered by the courts?
Professor Feldman: As far as I know, it never has.

Q540 ***Lord Woolf:*** I am not aware of it.
Professor Feldman: It would probably depend on some doctrine of necessity. It would be quite difficult to establish in those circumstances.

Q541 ***Lord Woolf:*** I dare say. We have now, I think, come to a situation where in this jurisdiction we adhere to a principle of separation of powers. Do you consider that the extent of the surveillance and data collection activities that are taking place have any impact on the separation of powers?
Professor Feldman: I do not think, my Lord, that it has any direct impact on the separation of powers, but the separation of powers may have implications for those kinds of activities. For example, in other jurisdictions where the separation of powers has long been a central constitutional principle—for example, the Australian Commonwealth—it has been held that warrants, when required to authorise interference with private space, or private lives, or interception of communications, must not be issued by a judicial authority because the issuing of warrants, the authorising of that sort of activity, is classified as an executive or ministerial act rather than a judicial act, and so it breaches the separation of powers to have it authorised by a judicial officer. That is something which we would, I think, find rather difficult in this country and rather strange, but it does raise questions about the extent to which one might want to look at the allocation of power, the nature of powers—executive, legislative and judicial—over authorisation processes for different kinds of surveillance or data collection. Secondly, take management or regulation of the storage and implementation of authorities; and then final decisions about the way in which the activity had been conducted, interfering with people's rights or breaches of legal obligations. The last of those is clearly a judicial function. I think it should ideally be carried out by a judicial authority. The first may or may not be; the one in the middle, I think, is not.

Q542 ***Lord Woolf:*** Do you see any need, in order to maintain the separation of powers, to make any particular agency of state power subject to restrictions on their surveillance and data collection powers?
Professor Feldman: Yes, my Lord, I see some really quite serious problems where there is a gap in the authorisation and so in the legal accountability for certain of these powers. I can draw attention particularly to two. One is the use by local authorities of—I come back to it again because I think it is a major gap—CCTV and similar surveillance and the use of the information that flows from that; and, secondly, responsibility for information sharing where a particular agency has quite legitimately exercised a statutory power to acquire or store personal information and then is given a very wide discretion as to the circumstances in which he can share that with others. Youth offending teams, for example, are a classic example of that, where although the person who originally held the information remains subject to Data Protection Act obligations in relation to the information, that person is also enjoined to share it with education or health professionals and it may well lead to a situation where it is not at all clear who is accountable or responsible for the use made by those further bodies. I would like to see something done about it.

Q543 ***Lord Woolf:*** Obviously, from what you have said, there are circumstances where you see a need for greater protection than we have already. From a constitutional perspective, who would you see as best placed to protect the constitutional rights in this area against over zealous surveillance and data collection? Should it be the role of Parliament or some other independent body or both? We have heard from the Commissioner.
Professor Feldman: Yes. I think the Commissioner does a very good job. I think that the question has to be answered in relation to the various elements in the collection and processing of data. It is clearly the responsibility of Parliament to establish, if possible, generally applicable criteria for bodies that are going to be given power to use powers to obtain information and then store and use it. The statutory regimes are at the moment rather a patchwork quilt. Each in its own terms is quite valuable and well thought out, although there are gaps, but I think that the legislature does need to look at the overall distribution of these powers and decide on the criteria—only Parliament can do that job—and introduce some sort of consistency into the picture. When it comes to the regulation of the powers that are granted, that seems to me to be outside the functions of Parliament, although the individual select committees of each House have a role in reviewing the use of powers, but on a day-to-day basis that has to be the job of the dedicated regulator, or regulators, and I think, on the whole, we are fortunate in the ones that we have. We may want

more and we may want to extend the jurisdiction of the ones we have to cover other areas.

Q544 ***Lord Woolf:*** Regulators rather than parliaments.
Professor Feldman: Regulators rather than parliaments. The idea of parliaments trying to carry out micro-management or micro-regulation of, and advice to, the work of people gathering and using information seems to me unrealistic now.

Q545 ***Lord Woolf:*** You obviously see a need on the larger plain for developments, I think is implicit in your answer, by Parliament. How could things be made more effective in scrutinising the Government's creation and use of surveillance and data collection powers?
Professor Feldman: I suppose that that could be done through orthodox techniques, by giving effect to individual ministerial responsibility for each House, by raising questions, taking evidence from ministers and their officials in the way that select committees do. That may well be useful, it may well be very useful, in working out what might be done where something has obviously gone seriously wrong in the Government's management of its data responsibilities through, for example, loss of large amounts of personal data, something of that kind. I think it is less effective where one is dealing with agencies outside the central government, simply because of the limited capacity to make ministers responsible for activities of outside agencies, and it is particularly likely to be ineffective where one is dealing with private individuals, private organisations that are using powers, as is happening a great deal. Now I think one relies on a regulator operating outside Parliament.

Q546 ***Chairman:*** Before turning to Viscount Bledisloe, can I jump back briefly to the separation of powers? You mentioned the position in Australia. The Committee is going to be taking evidence in the United States later in the month. Do you think that the interception authorisations by the judiciary in the United States, the judicial authorisation interceptions, breach the separation of powers?
Professor Feldman: One of the things about the separation of powers is that it is, like any other constitutional principle, to be interpreted in the light of the constitutional arrangements in a particular state. I think that we would not say in this country, traditionally we have not said, that the issuing of authorisation, for example, to search premises by a magistrate or, indeed, by a county court or high court judge breaches the separation of powers because we have a different view both about the separation of powers and about the classification of that function as judicial or ministerial; so I think whether it breaches the separation of powers in the USA will depend on the view taken by the USA of its own constitutional separation of powers and can only be seen in that context. I would not want to try to import it any more than I would want to try to import the Australian model.
Chairman: I think, Professor Feldman, you ought to be a politician.

Q547 ***Viscount Bledisloe:*** Is it right that, in so far as the collection of personal data is concerned, the private sector is less constrained than the public sector, for example, because Article 8 does not apply to the private sector?
Professor Feldman: Yes and no, my Lord.

Q548 ***Viscount Bledisloe:*** The "yes", I can understand. Could you explain the "no"?
Professor Feldman: The "yes", as you have said, the Human Rights Act and the obligations that are imposed directly by Article 8 of the European Convention do not apply other than to public authorities. The "and no" is slightly more complicated than that, first because the European Convention on Human Rights as interpreted by the Strasbourg courts imposes on states positive obligations, which include in some situations obligations to regulate the activities of private individuals or bodies to ensure that they do not do something which impacts on other people's Convention rights, and it is through that kind of indirect mechanism that the courts in this country have been able to develop, for example, the law of breach of confidence in ways that give protection to some Article 8 interests that would have been undreamed of 15 or 20 years ago. The other side of the "and no" is that the Data Protection Act applies to private as well as the public users of personal data. There is no distinction there, and in some ways you might say that, as far as that Act is concerned, the constraints on private users of information are stronger than those on at least some public agencies because the private agencies are less likely to be able to make use of the limitations on their obligations, for example cases involving protection or prevention of crime or protection of national security or the exercise of regulatory functions.

Q549 ***Viscount Bledisloe:*** In the light of that, do you see a worry and a danger in the sharing of personal data which has been collected in the private sector with the public sector or vice versa?
Professor Feldman: There is a significant risk that, where information is collected by the private sector for the business purposes of private sector organisations and is then shared with the public sector, the person who provided the information will not know and will not be able to find out, first, that

the information is being shared and, second, that it is being used by the other agency for a purpose completely different from that for which the information was originally provided. What is effectively able to happen is that information which is provided by a person for the purposes of that person ends up being used by a completely different agency for purposes that they may be either not for the benefit of that person or directly contrary to the interests of that person. For that to happen without some clear process of authorisation and decision-making and perhaps information being given to the data subject is a matter of concern, and it operates *mutatis mutandis* in the other direction as well.

Q550 ***Lord Rowlands:*** I think on a number of occasions you have touched on the role of Article 8 as a good basis for the protection of privacy rights. Do you think the exemptions in Article 8(2) are too broad, and, if so, in which way would you restrict them?
Professor Feldman: I think the exemptions in Article 8(2) are in themselves perfectly satisfactory, but we come back to the point that was raised in my Lord Chairman's question, I think, earlier about whether proportionality is a satisfactory basis for protecting rights. I have no problem with any of the legitimate aims that might justify an interference with the rights under Article 8(1). I think, in fact, that one needs fairly broadly stated legitimate aims for two reasons: first, privacy related rights are inevitably the subject of suspicion that they can be used for illicit or improper purposes, and so the possibility of control or limited interference over a wide range of purposes is quite sensible; second, because the European Court of Human Rights has interpreted the scope of the right in paragraph (1) of Article 8 so incredibly broadly as covering more or less now any aspect of any person's personality or life-plan, that for practical purposes one almost never sees the Strasbourg court say, "This interest, which is asserted as an Article 8 interest, actually falls outside Article 8". The whole focus, therefore, has been on the justification for interfering with the rights under Article 8(2), and where one has an immensely wide set of rights, then it makes sense to have a similarly flexible and adaptable set of justifications potentially for interfering with the right. The core of the question is how robustly do, first of all, initial decision-makers, and then reviewing commissioners, tribunals or courts apply the pressing social need for the interference and proportionality of the interference tests, because that is crucial? If it is done robustly and with careful attention to the detailed circumstances of each case, as it is done typically by the Information Commissioner and the Information Tribunal, then it works well. As I said earlier, the more one allows an attitude to creep in that one will, other things being equal, assume that the decision-maker made a sensible decision, the less effective it will be and the more need there may be to put some extra tension into the way that the Article 8 right is—

Q551 ***Lord Rowlands:*** Just completing what you are saying, you do not think we should try to redraft Article 8(2), but it is in the application. Has the experience to date shown that in fact this balance has been generally speaking held, the kinds of tensions you have described have produced sensible and reasonable outcomes?
Professor Feldman: On the whole, I think the answer is, yes. In fact, the Strasbourg court has shown an interesting tendency to be very critical of the use particularly of personal information and photographs by state agencies. For example, it has held that it breaches Article 8 and it is a disproportionate interference with Article 8, without a special reason, to publish photographs of people who have been arrested and charged with criminal offences in the case of *Sciacca v Italy*. It has also been held in Strasbourg that the state, Germany in this case, was unable to justify a gap in its constitutional law in the protection for privacy of the individuals against having photographs of those individuals published in the press even where the individuals concerned might be described as public figures; so it means that you are seeing at the Strasbourg level pretty strong attention to the impact on individuals of particular forms of interference with—

Q552 ***Lord Rowlands:*** The political test will be the DNA cases.
Professor Feldman: Yes, exactly, which I am looking forward to greatly.

Q553 ***Lord Peston:*** I am still a little puzzled about the human rights aspect of the concept of the purpose for which the data was collected, which you have referred to several times. To take one within my own field, which is economics, we fill out a tax form for the purpose of the Government taxing us, but that data, as I understand it, becomes the basis for calculating national income as part of the large input into that kind of calculation, and there are many other examples of that without which there would not be the massive economics data economists rely on in order to do their subject. What would happen? Is there a human right in your concept of you saying, "I do not want my tax form to be used in calculating national income"? Most people would regard that as crackers, and yet your concept of purpose seems to me to lead to that being a valid position that you could take. I am just a little puzzled. I honestly do not see your human rights being infringed very strongly by ONS being able to calculate national income via,

partly, what the Revenue tells them is coming through from the tax form.
Professor Feldman: I agree.

Q554 ***Lord Peston:*** I am prejudiced here because I want to defend the ability of economists to do their subject.
Professor Feldman: You are right to defend their subject. I think the answer is that one has to look at the form in which the information is used. When we fill in our tax returns, the information is clearly personal: it relates to identifiable individuals and is used for the purpose of calculating the tax due from those individuals; but one can both anonymise and aggregate information in ways that make it cease to be personal information. At the point where it is anonymised and aggregated, the information ceases to be personal information because it is not capable of being used to identify anything relating to a particular individual. At that point there is no reason why it should not be used for calculating national income or, indeed, anything else. It has to be said that we are already a great deal less protective of personal confidentiality in the tax system than we were 210 years ago when income tax was first introduced, because the schedule system for income tax was originally introduced so that each schedule, or income under each schedule, was returned to a different inspector so no one person ever knew the total income of any person, and that was the purpose of the schedule system.

Q555 ***Chairman:*** One of the purposes.
Professor Feldman: It got undermined when the basis for income tax moved to total income in the early seventies.

Q556 ***Lord Peston:*** So we protect your human rights by aggregation and anonymity.
Professor Feldman: Yes.

Q557 ***Lord Peston:*** Our pledge to you then is that that is what we do, and sometimes we may fail.
Professor Feldman: Yes, the same applies in other contexts: the aggregation and anonymisation of medical information that is needed for health planning and statistics.

Q558 ***Baroness O'Cathain:*** Does the existing law of breach of confidence compensate for the deficiencies of Article 8? Is privacy better protected through the tort of breach of confidence?
Professor Feldman: It depends on what you think the deficiencies of Article 8 are, but my view of that is as follows. As a matter of domestic English law, leaving aside completely the statutory regimes of the Data Protection Act and the human rights regime, the only credible candidate for protecting privacy as a matter of domestic common law was breach of confidence, but breach of confidence protects only particular types of privacy. It protects privacy in relation to information and there has to be something in the nature of the information which makes it of a kind that makes it sensible to be regarded as confidential. A lot of the constraints around the use of breach of confidence have been relaxed by the courts, and Lord Woolf in his judicial role made a substantial contribution to the development of breach of confidence in that way, but it still remains, essentially, an information-based remedy. It is very difficult to use it to deal with the process of acquiring or collecting information through general surveillance, for example, because much of what is collected simply would not be regarded, even arguably, as confidential even though it might be an important aspect of people's ordinary private lives. Nor does it provide a basis for giving protection against harassment as such. All of that relies on other statutory regimes and Article 8 of the European Convention. I think my answer to your Ladyship's question is that I see breach of confidence, as developed in the light of the Human Rights Act, as a useful hand-maiden to the protection of privacy of information, but not as something that could ever take the place of Article 8 or the other statutory regime.

Q559 ***Baroness O'Cathain:*** As a supplementary to that, do you think the development of a separate tort of privacy would help to protect the privacy interests of individuals and organisations?
Professor Feldman: If we could do it, it would help. It would have, I think, now to be done by statute, as I think the courts have effectively painted themselves out of the picture by a number of decisions which, with respect, I found slightly disappointing, but the ultimate one, in a case *Wainwright v Home Office,* which simply reaffirmed the absence of a privacy right at common law, means that for practical purposes we are going to depend on legislation and the Human Rights Act.
Viscount Bledisloe: I think that last answer has very clearly and concisely answered my question. Lady O'Cathain having volunteered to ask it has meant that I do not need to.

Q560 ***Baroness Quin:*** My question has also been touched on to a certain extent, because you did mention earlier on some good aspects of RIPA and also the Data Protection Act. Nonetheless, perhaps you should be given a chance to add anything that you have not added before. Do you think that the surveillance powers currently granted to the state are too broad overall, and does the existing regulatory regime, created by legislation such as the Data

Protection Act and RIPA, provide adequate safeguards and restrictions?

Professor Feldman: The first part of the question, the breadth of the powers, I think, is a very difficult one for me to answer, because it is essentially, I think, a political question rather than a legal one. Agencies need powers to some extent. Particularly when one is dealing with investigative and security agencies, one is dependent on their account of the powers they need to decide whether they are too broad. The exception, I think, is if they seek a power which is one which is simply unacceptable on fundamental principles in any humane society. A power to torture, for example, would, in my view, fall into that category, and a power to detain people for very long periods without any charge would also fall into that category, but leaving aside those sort of fundamentally unacceptable powers, it seems to me, ultimately, to be a question for political judgment what powers should be given. The second part of the question, relating to the safeguards provided by regulatory regimes we have, I think is much easier for me to say something about. The RIPA and Data Protection Act regimes are, as I suggested earlier, fairly well nuanced in terms of the powers that they grant. The powers are identified under RIPA. One has the targeted surveillance, the intrusive surveillance and the covert intelligence sources by different agencies, different criteria for using the powers applied under statute in relation to each of those powers. What I think might need further attention is the authorisation method that is contained in the statute. In relation to the use of those powers—certainly targeted surveillance and use of covert intelligence sources—those are left to be authorised by senior officials within the agencies. When one gets to intrusive surveillance, in relation to the police and other agencies, but not the security and intelligence services, the Surveillance Commissioner has to approve in advance or retrospectively. In relation to the Intelligence Services there is a secretary of state authorisation which is not subject to the Surveillance Commissioner's review, but in relation to all of those there is then a subsequent opportunity to complain to the Investigatory Powers Tribunal, which has jurisdiction. I think the Investigatory Powers Tribunal has yet to prove itself—it has not had enough to do yet perhaps to be clear just how effective it is going to be—but I am a little bit worried about the extent to which these intrusive or relatively extensive activities can be authorised by a senior official of the agency that is going to carry out the activity without the need for external independent scrutiny in all cases.

Chairman: Professor Feldman, the time is sadly marching on. We have time for one brief final question from Lord Peston.

Q561 ***Lord Peston:*** Just to make clear your view: if Parliament grants powers to anybody of the sort that you are talking about, is it not the case that it is likely that whoever has been granted those powers will always use them over zealously because the consequences are not symmetric? Over zealousness, the noise of the odd individual personal, and so on. Under zealousness leads to a building blown up, people killed and that sort of thing, and I am not very clear in your answer to Lady Quin's question what Parliament can do, or anybody can do, to get rid of that asymmetry? Parliament can say, "These are the powers. We want them used properly", but the fact is that the bias is in that one direction rather than the other and I do not see how Parliament, or the regulator for that matter, could solve that problem?

Professor Feldman: I think, Lord Peston, I agree with that. Any system of control which relies on decision-making by a whole range of people in an organisation or series of organisations will only work as well as the people who are operating it allow to it work. As you say, people in a lot of these situations tend to be risk-averse, and understandably so. One can try to create a climate, through political and managerial means, where risk-aversion becomes the exception rather than the norm but it will always be around somewhere, but what I would say is this. It is better, I submit, to have a system in which the criteria that you want to have applied are clear and the circumstances in which they are to apply are clear and have, ideally, legal authority behind them, so that you can take some kind of action if it turns out that they have been misused or abused, than a situation in which the powers are unclear or left entirely to the discretion of the decision-maker, in which case accountability becomes extremely difficult and there will be a temptation to stretch things ever further on the part of the people operating the powers.

Chairman: Professor Feldman, thank you very much indeed for joining the Committee and for the evidence you have given, which has been extremely interesting for all of us. We are deeply grateful.

WEDNESDAY 14 MAY 2008

Present	Bledisloe, V	Peston, L
	Goodlad, L (Chairman)	Rodgers of Quarry Bank, L
	Lyell of Markyate, L	Rowlands, L
	Morris of Aberavon, L	Smith of Clifton, L
	O'Cathain, B	Woolf, L

Memorandum by Dr Victoria Williams[1]

SUMMARY

The Information Commissioner has recently repeated calls for Privacy Impact Assessment (PIA) to be required before new surveillance technologies are introduced. In evidence to the Home Affairs Committee inquiry entitled "*A Surveillance Society?*" he has referred to models of PIA in common law jurisdictions including under the US E-Government Act 2002. In this submission it is argued that to apply concepts of PIA to public places requires more than merely importing the model of personal data privacy and requires consideration of the impact on society, but that we have to be wary of introducing excessively subjective concepts. Entering public space leads to issues such as freedom of association and of speech becoming more relevant than data privacy alone.

It is concluded that if PIA is to be applied to new surveillance projects, consideration needs to be given to procedural requirements for publication and review linked in some way to planning or budgetary approval by analogy with the US E-Government Act arrangements which link budget with PIA compliance.

It is suggested that by analogy with US civil liberties law it will be necessary to consider whether technologies which observe public space ought to be rebuttably presumed to create a risk of "chilling" the free exercise of rights of association and free expression protected by Articles 10 and 11 of the Convention, for the purposes of scoring the societal impact of surveillance during the PIA process. The law makers need to engage in significant Constitutional review of the basis on which the State and similar bodies are permitted to observe people in public space and what rights to freedom from surveillance the public have in respect of social activity in that space, before it will be practical to attempt to assess the impact of surveillance.

1. I am grateful for this opportunity to present this submission to the Committee. These observations have as their backdrop the recently renewed calls by the Information Commissioner for Privacy Impact Assessments (PIA's) similar to those required for data collection systems in some other jurisdictions such as under the US E-Government Act 2002, to be carried out prior to the use of what the Commissioner called "initiatives and technologies which could otherwise accelerate the growth of a surveillance society".[2] The Commissioner's reference to "new surveillance technologies" comes at a time when all of the following are available technologies:

- Unmanned Aerial Vehicles ("drones") for law enforcement;[3]
- computer face recognition[4] and detection and automated tracking of suspicious behaviour;[5]
- "speaking" CCTV[6, 7] and street furniture with localized sound recording capabilities;[8]

[1] The author is member of the Bar and is the author of *The Surveillance and Intelligence Law Handbook*, Oxford University Press (2006). This evidence is submitted on a personal basis and not on behalf of any corporate or representative body.

[2] Office of the Information Commissioner, "*Information Commissioner calls for new privacy safeguards to protect against the surveillance society*", Press release 1 May 2007.

[3] "Police test drone spy helicopters", BBC News 21 March 2007. See http://news.bbc.co.uk/1/hi/england/merseyside/6477831.stm

[4] "Facial recognition software is used to automate perjury charges for those attempting to challenge speed camera tickets". *The Banbury Guardian* 12 October 2006 http://www.banburyguardian.co.uk/ViewArticle.aspx?SectionID=687&ArticleID=1817997

[5] "CCTV camera 'tails' suspects", *Times*, 16 April 2007, http://www.timesonline.co.uk/tol/news/uk/crime/article1655200.ece

[6] "Talking CCTV gives Big Brother a voice", *The Telegraph* 5 April 2007, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/04/04/ncctv104.xml

[7] "Talking CCTV cameras accuse wrong person", *Guardian* 12 April 2007, http://www.guardian.co.uk/humanrights/story/0,,2055082,00.html

[8] "Council plans to listen in on street life", *The Telegraph*, 4 May 2005. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/05/04/nmic04.xml&sSheet=/news/2005/05/04/ixhome.html

— networked CCTV operated equipment able to speak to and then if necessary disable targets with non-lethal force; and[9, 10]

— Radio Frequency Identification (RFID) technology capable of scanning identity documents within a few metres,[11] or when moving in wifi networked areas.[12]

2. Before the recent calls for PIAs the issue had been canvassed in the context of the National Identity Register and ID Card scheme, in the form of a proposal that the government should be under a duty to commission and publish the results of PIA's as and when details of information appearing on the face of the ID card were proposed by way of legislation.[13]

3. In some contexts in the UK the PIA is seen as good practice on a voluntary basis. The Department of Constitutional Affairs (now the Ministry of Justice) promoted the use of PIA's in the context of public sector data sharing. Its response to consultation on the Government paper "Privacy and Data-sharing: the way forward for public services", recommended that "Where appropriate, organisations should use . . . Privacy Impact Assessments, to initiate an open dialogue with the public and with stakeholders around new data-sharing initiatives".[14]

4. Acceptance of the appropriateness of PIA is more limited when one turns to the context of the high-profile National Identity Scheme and the ANPR[15] project. The Secretary of State's recently stated position[16] was that no privacy impact assessment had been produced, or was planned, for either system.

Privacy Impact Assessment & Surveillance

5. The final "Surveillance Society" report commissioned for the International Data Protection and Privacy Commissioners' Conference provided a composite definition of Privacy Impact Assessment:[17]

— "'an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated';[18]

— 'a process. The fact of going through this process and examining the options will bring forth a host of alternatives which may not otherwise have been considered';[19]

— an approach and a philosophy that holds promise by instilling a more effective culture of understanding and practice within organisations that process personal data;

— a form of risk-assessment, which therefore cannot escape the uncertainties of identifying and estimating the severity and likelihood of the various risks that may appear, to privacy, life-chances, discrimination equality and so on;

— a tool for opening up the proposed technologies or applications to in-depth scrutiny, debate and precautionary action within the organisation(s) involved;

— like PETs,[20] premised on the view that it is better to build safeguards in than to bolt them on;

— an early-warning technique for decision-makers and operators of systems that process personal information, enabling them to understand and resolve conflicts between their aims and practices, and the required protection of privacy above or the control of surveillance; and

— ideally, a public document, leading to gains in transparency and in the elevation of public awareness of surveillance issues and dangers may be realised; in turn, it may assist regulatory bodies in carrying out their work effectively".

[9] ". . . Once an engagement decision is made (either by the operator or the system depending on user selected settings), the unit will then arrest the targeted individuals by providing complete incapacitation" at http://www2.taser.com/products/military/Pages/TRAD.aspx
[10] ". . . a New Deterrence Camera with Non-Lethal Incapacitating Capabilities" at http://www.icxt.com/news/view.cfm?content_id=7BACAB87-F70B-1CB5-EB94B75B2AEA8C6B
[11] Parliamentary Office of Science and Technology "Postnote" July 2004 No 225, available at www.parliament.uk/documents/upload/POSTpn225.pdf
[12] "Wi-fi and RFID used for tracking", BBC 25 May 2007 at http://news.bbc.co.uk/1/hi/technology/6691139.stm
[13] Office of the Information Commissioner,"The Identity Cards Bill—the Information Commissioner's Perspective", 2005.
[14] The Lord Chancellor's Department, Recommendation 19 of "Analysis of responses to the consultation on the Performance and Innovation Unit report '*Privacy and Data-sharing: the way forward for public services*'", March 2003.
[15] Automated Number Plate Recognition.
[16] *Hansard* 8 February 2007 : Column 1090W.
[17] At para 45.1.2 of the report.
[18] Stewart, B. (1996) "Privacy impact assessments". Privacy Law & Policy Reporter 3 (4): 61-4.
[19] Stewart, B. (1996) "PIAs—an early warning system". Privacy Law & Policy Reporter 3 (7): 134-8.
[20] Privacy Enhancing Technologies, see for example "Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs)", Office of the Information Commissioner 11/4/06.

The US E-Government Act 2002[21]

6. The Information Commissioner's recent suggestions refer to the position in overseas jurisdictions such as the USA where the PIA process is mandatory in data collection contexts under the E-Government Act 2002. In US law a PIA is described as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks".[22]

7. The 2002 Act sec 208(b)[23] creates legal obligations for the production of PIA's in relation to government agency IT systems, but the principle may be capable of expansion to surveillance systems, as advocated by Professor D Mulligan, of UC Berkeley School of Law in submissions to the Department of Homeland Security Data Privacy and Integrity Advisory Committee in June 2006,[24] and canvassed in the "Surveillance Society" report itself.

8. Before doing either of the following activities (the first of which is perhaps most relevant here), under US law a government agency comes under several obligations in relation to production of PIA's. The activities which trigger the PIA obligation are:

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form, or

(ii) initiating a new collection of information that will be collected, maintained, or disseminated using information technology; and which includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

9. The PIA obligations

In circumstances where the obligation is triggered, ie under (i) or (ii) above, each agency is obliged to:

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. The requirement to make the PIA publicly available may be varied or waived for security reasons or to protect classified, sensitive, or private information contained in the PIA.

10. The filing of the PIA forms part of the funding process. Agencies must, where a PIA is required by the Act, provide the Office of Management and Budget with the PIA for an information technology system for which funding is sought.

The Adequacy of Privacy Impact Assessment and of Article 8 in Public Surveillance

11. Whilst in general citizens expect privacy in the sense that they will not usually be eavesdropped upon or observed by the State in our own private spaces, it is trite to say that the very act of appearing in the town centre or travelling between locations brings with it a different expectation. In many contexts that may be the whole point of the exercise; perhaps even deliberately in order to be captured on CCTV.[25] The presence of CCTV has been said to be comparable in character to the presence of an individual observer.[26] An argument supportive of the general observation of public places by the State using technological means is that any person

[21] for an in depth discussion of the relative merits of US and European approaches to information privacy laws in general, see Biginami, F, (2007) "European versus American liberty: a comparative privacy analysis of antiterrorism data mining", Boston College Law Review, 48:608, see eg (as to PIA) p 697. Available at www.bc.edu/schools/law/lawreviews/bclawreview/meta-elements/pdf/48_3/03_bignami.pdf

[22] US: Office of Management and Budget Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Annex A part II(A)(6).

[23] US: E-Government Act of 2002, Pub L No 107–347, 17 December 2002.

[24] Available from the University of California at Berkeley, via http://www.law.berkeley.edu/clinics/samuelson/expectations.html

[25] An interesting example, which doubles as an example of the modification of public behaviour by CCTV, being the "The New York Surveillance Camera Players" performing adapted plays in front of security CCTV in the New York area, in protest against surveillance technology, referred to in Greenhalgh, S, (2003), Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour (Aug. 2003), http://www.oipc.ab.ca/ims/client/upload/LitReview.pdf

[26] "A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character" (*PG and JH v UK*, ECHR judgment 25 September 2001, Application No 44787/98 at 57).

going about his or her business openly is well aware that anyone else can see or hear them and that the State is no different from the citizen in terms of its right to watch a general scene, subject to the existing law of data protection. Thus in *Peck v UK*[27] the ECHR reiterated that "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life". It is clear that the extent to which recording surveillance material fails to respect Article 8 rights is itself dependent largely on factors such as the context of the recording, the use to which it is put and the legal reasons for it.

12. At the root of the present debate over surveillance technology, and calls for PIA to be extended to it, appears to be not merely concern over the collection of conventionally personal data but also concern over the impact which mass surveillance may have on society. The Commissioner in evidence to the Home Affairs Committee inquiry stated at para. 5:

> ". . . the Commissioner's concern is to ensure that full consideration is given to the impact on individuals and society [. . .]. The issues are complex, difficult and controversial. They raise questions about the nature of society, about the role of the state, about the activities of commercial bodies and the about the autonomy of citizens".

13. To encapsulate such concerns within a framework for surveillance PIA seems to require that we develop a clearer idea of the extent to which, if at all, society and its democratic activities of free speech and assembly ought to be protected from State surveillance. It also requires that we know what we mean by "impact" in that context, as opposed to impact in the context of solely personal data privacy. There is a risk of recourse being had to philosophically valid but practically difficult questions such as such as "What . . . a new audio-visual scheme for monitoring public places or private shopping precincts, implies for personal autonomy and dignity, social solidarity, or the texture of social interactions".[28, 29]

Rights of Free Speech and Free Association Under Articles 10 and 11

14. In the United States the courts have recognized that citizens should be able to remain anonymous *vis a vis* the State whilst in the course of exercising certain constitutionally protected social rights, most notably rights to free speech and freedom to associate. It is unconstitutional for a law to require those who wish to canvass religious material door-to-door to have to identify themselves to the authorities via a broadly applicable permit scheme.[30] Moreover the US courts also recognize that a law which has the effect of discouraging the exercise of constitutionally protected rights may itself be struck down:[31] the so called "chilling effect" which has to a degree also been recognized in European human rights especially in the context of Article 10 (freedom of expression) (eg *Steel and Morris v UK* and *Steur v Netherlands*).[32]

15. The extent to which US Constitutional rights such as those under the First[33] and Fourth[34] Amendments may be infringed by public observational surveillance remains, it appears, an uncertain matter in terms of decided case law,[35] but the arguments under US law were aired to a degree in *Vo v City of Garden Grove et al*[36] in which the Court of Appeal of the State of California refused to hold that an ordinance requiring the placement of CCTV[37] in "cyber-cafes" affected First Amendment (free speech) activity any more than did the legitimate presence of a security guard, nor was there any legally protected privacy interest. (Though it was accepted that the ordinance in question did at least implicate First Amendment rights). The Vo judgment was subject to one very strongly worded dissenting judgment by Sills, J expressing the view that the Ordinance "literally forces a 'Big Brother' style telescreen to look over one's shoulder while accessing the Internet".

[27] *Peck v UK* ECHR App No 44647/98 (23 January 2003) at para 59 referring to *Herbecq and Another v Belgium* (App No 32200/96, decision of 14 January 1998).
[28] ibid, 45.2.4.
[29] GT Marx poses a set of 29 questions to be asked when considering the ethics of particular surveillance projects, and one might relatedly envisage impact checklists or instruments designed to reduce the risk of excessive subjectivity or abstraction as part of a surveillance PIA. Marx, G T. (1998), An Ethics For The New Surveillance, The Information Society, Vol 14, No 3, 1998. Also reproduced as Appendix 3 to the "Surveillance Society" report.
[30] See *Watchtower Bible & Tract Society of N.Y., Inc v Village of Stratton*, 536 U.S. 150 (2002) and (on freedom of association without identification), *NAACP v Alabama*, 357 U.S. 449 (1958).
[31] eg *Lamont v Postmaster General*, 381 U.S. 301, 303 (1965).
[32] *Steel and Morris v UK* ECHR application no. 68416/01 and *Steur v Netherlands* ECHR application No 39657/98.
[33] Freedom of speech and association, freedom of religion, etc.
[34] Freedom from unreasonable searches and seizures, etc.
[35] An interesting discussion appears in Mulligan, D, (June 2006) submissions to the Department of Homeland Security Data Privacy and Integrity Advisory Committee, text available from the University of California at Berkeley, via http://www.law.berkeley.edu/clinics/samuelson/expectations.html
[36] *Vo v City of Garden Grove* (2004) 115 Cal.App.4th 425.
[37] which was required to be "capable of delineating on playback . . . the activity and physical features of persons or areas within the premises"

16. In terms of ECHR case law under Articles 10[38] and 11,[39] at least where unjustified interference with rights under Article 8 is also shown, it appears to have been accepted in principle that keeping files about a person's political activities, gained from "surveillance" in a broad sense (including for example keeping newspaper cuttings on file) can amount to a violation even in the absence of direct evidence that there is a practical impact on the practical exercise of those rights. In *Segerstedt-Wiberg and others v Sweden*,[40] the ECHR was prepared to rely upon the fact that it had found a violation of Article 8 as implying a corresponding violation of Articles 10 and 11, stating that (at para 107): "the storage of personal data related to political opinion, affiliations and activities that is deemed unjustified for the purposes of Article 8 § 2 ipso facto constitutes an unjustified interference with the rights protected by Articles 10 and 11".

17. The Judgment in Segerstedt-Wiberg does not consider whether there could be circumstances where surveillance which did not also infringe Article 8 might nonetheless infringe Articles 10 and 11, absent proof of practical interference with (or penalty imposed for) exercise those rights. However the decision does at least suggest that rights of expression and of association could be infringed by the mere storage of surveillance information, presumably more especially so if "chilling" effects were to be plausibly suggested.

18. There is a dearth of empirical research evidence as to the impact, if any, which surveillance has on the actual exercise of rights of free speech or free association by citizens. Politically the principle that the monitoring of assembly is to be avoided was propounded in the "Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society" in the context of protecting Article 11 rights in cyberspace. There appears to be no principled reason to believe that the same idea is irrelevant to "real space" assembly:

> "Member states should adapt their legal frameworks to guarantee freedom of ICT[41]—assisted assembly and take the steps necessary to ensure that monitoring and surveillance of assembly and association in a digital environment does not take place, and that any exceptions to this must comply with those provided for in Article 11, paragraph 2, of the ECHR".[42]

Conclusions

19. The conclusions which I suggest can be drawn from the above when we try to adapt PIA to surveillance contexts fall into two categories:

(i) matters of practice and procedure in relation to possible mandatory PIA, based on models such as the E-Government Act 2002, insofar as those can be adapted to surveillance contexts;

(ii) matters of law and principle in relation to the framework of rights to privacy by which the "impact" in a Privacy Impact Assessment of public surveillance may be gauged.

20. (i) Matters of practice and procedure

As to (i) it seems to this author that "surveillance" PIA would risk becoming mere paperwork unless linked to a clear set of requirements for:

— publication;

— review;

— approval by a competent authority; and

— a link between adequate PIA approval and planning, regulatory or funding decisions.

21. It would appear less than ideal for a surveillance PIA exercise to be required in the absence of any scope for practical control. The linkage between PIA and budgeting under the E-Government Act 2002 may perhaps be seen as an example of such practical control.

22. (ii) Matters of law and principle to be applied in PIA for surveillance contexts

As to (ii) it suggested that an extension of PIA to cover surveillance requires more than mere procedure. It requires that the legislature develops a clear set of principles to be applied to assessing the social impact, rather than merely the personal data privacy impact, of public surveillance. Failing to do so would risk a "surveillance PIA" which adds little to existing personal data privacy safeguards.

[38] Freedom of expression.
[39] Freedom of assembly and association.
[40] Application no 62332/00, ECHR Chamber judgment 6 June 2006.
[41] Information and Communication Technology
[42] Committee of Ministers CM(2005)56 final 13 May 2005, Council of Europe https://wcd.coe.int/ViewDoc.jsp?BackColor Internet = 9999CC&BackColorIntranet = FFBB55&BackColorLogged = FFAC75&id = 849061

23. Whilst the rights to respect for private life, home and correspondence in Art. 8 of the Convention, and the provisions of the data protection legislation provide a basis for a right to protection from abuses of personal data privacy whether in private places or outdoors, conventional notions of privacy impact do not translate well into public behavioural settings where observation may be thought to affect or chill the exercise of other more social rights, which more or less presuppose a public or semi-public stage upon which the individual appears.

24. The conclusion drawn here is that the lawmakers should carry out an exercise of constitutional review as to whether the law ought to presume (axiomatically) that systems which observe public places create a risk of chilling the exercise of rights such as free speech and free assembly. That would require consideration whether surveillance which impacts, or has the potential to impact upon, anonymity in social space would lose points on social impact grounds, rather than purely personal privacy grounds, in a surveillance PIA. It would also require consideration as to whether greater constitutional protections than exist at present are required for free speech and association rights in public places, independently of purely personal data privacy protections.

1 June 2007

Examination of Witness

Witness: Dr Victoria Williams, examined.

Q562 ***Chairman:*** Good morning, Dr Williams. May I welcome you very warmly to the committee and thank you for submitting your written evidence in advance. As we are being recorded, could you identify yourself for the record?
Dr Williams: I am Dr Victoria Williams and I am a member of the Bar.

Q563 ***Chairman:*** Would you like to make a short opening statement to add to your written submission or not?
Dr Williams: I am quite happy to go to questions. I have obviously handed in quite a lengthy submission.

Q564 ***Viscount Bledisloe:*** I wondered if you wanted to qualify or add to anything that you had said in the light of the J K Rowling judgment, assuming for the moment that it is right and upheld, so to speak. I do not mean upheld on appeal but that when the case actually comes on it is upheld?
Dr Williams: Yes, I would. I made a point of reading that yesterday. It is a judgment of course that was given on appeal from the striking out decision.

Q565 ***Viscount Bledisloe:*** Yes. That is why I say let us assume for the moment that it stands.
Dr Williams: Assuming that it becomes substantive, I believe it is very significant in the context of what might be described as the reasonable expectation of privacy in a public place. There is a part of the judgment where the court considers that it is at least arguable that when going about one's business, at least as a child, in public but carrying out a private matter, such as going shopping, one does benefit from at least a reasonable expectation that one will not be photographed and then have those photographs used. That is, as I see it, an extension of the existing principle, which was that if you were photographed for example with a long lens at a private function, perhaps over the wall of your garden from a tree, that would be protected, but this does appear to be an important extension and perhaps the beginning or the first judicial building block towards a more generalised right of public privacy, if I can put it that way.

Q566 ***Lord Morris of Aberavon:*** If that is upheld, it is going to be a very valuable and important extension to a law of privacy, is it not?
Dr Williams: I believe it would be. The qualification of course is that on the facts of that case it related to an infant child. The Court of Appeal was careful to make it clear that those were the specific facts of the case and that perhaps the adults would be in a different position, but, nonetheless, it is an important decision. It does point potentially towards, as I say, the beginnings of a judicial expansion of a right of privacy in a public space.
Lord Morris of Aberavon: On the facts, it might not apply to a minister of the Crown carrying papers openly to No. 10.

Q567 ***Chairman:*** In your written evidence, Dr Williams, you said, and I quote, "law makers need to engage in significant constitutional review of the basis on which the state and similar bodies are permitted to observe people in public space and what rights to freedom from surveillance the public have in respect of social activity in that space". Could you say what is the difference between the legal and constitutional issues that are engaged in the surveillance of a public space and those that are engaged in respect of the collection of personal data?
Dr Williams: Yes, and I should start by saying really that this issue is quite a philosophical one and necessarily there are overlaps, but as I see it probably the most obvious practical difference—one has to start with practicalities I think before one moves to legal matters—between public and private surveillance, if I can put it that way, is that public

surveillance operates on the space; it does not operate on the individual. CCTV, for example, watches the entirety of the town square. It is like fishing with a large net; you catch whatever passes through that space indiscriminately. Personal data collection and personal surveillance is more like fishing with a fishing rod; you are going for the individual fish that is identifiable. The bridge between those two domains of course is when you extract from the bigger net the individual and you extract their personal data from that. As things stand, in the domain of public surveillance, as I see it, the law does not currently appear, subject to the *Murray* case or the J K Rowling case as it will probably become known, to have developed a set of principles that deal with or can accommodate the idea that mass surveillance could have implications for the fabric of society itself and for the exercise of constitutional rights, such as free speech or free association and so on. The current framework deals only in terms of private rights and is essentially lacking in the notion that when people gather together in public there might be a public interest in having protected spaces or having any presumption that you may gather in public space without being watched by the state. I think that raises the constitutional question of whether we have sufficient safeguards for Article 10 and Article 11 rights at the moment—the rights of freedom of assembly, the rights of freedom of speech and so on—and those are as distinct from personal data privacy protections.

Q568 ***Lord Lyell of Markyate:*** The public and private distinction is interesting in the court context where the citizen brings a court case, but much more chilling is the idea, for example, that your conversations might be picked up by a parabolic microphone; that this might be done at the instance of the state; or it might be done at the instance of a business competitor; or at the instance of a newspaper, which was hoping to show that you were gay or something of that sort. Ought that simply to be left to supervision by the courts or ought there to be some actual legislation which governs who is entitled to do that kind of thing at all?
Dr Williams: Of course at the moment we have some legislation. There is data protection legislation, there is the Regulation of Investigatory Powers Act legislation, but what we do not have, as I see it, is an overarching set of fundamental principles laid down by Parliament, which will govern mass surveillance in that context. There seems to be something of a free-for-all at the moment, save when one starts extracting personal data. I have reviewed some of the technologies that are currently available at the start of my evidence: things like CCTV that can listen, CCTV that can even arrest the subject remotely by tazering them essentially based on computerised decision-making. Of course, we already live in an environment where as one walks through the City of London of course one's face is recognised; one's number plate is routinely recognised. Whether or not that data is processed, it is still there in the system and it could still be processed. I do suggest that the sheer scale of that mass surveillance could in itself have a chilling effect on the exercise of public rights. It could also lead to misuse of course if it fell into the wrong hands. Of course, the more data that one gathers, the greater the chance of error, which is always the possibility, or mistaken identity. The more one automates decision-making, the greater the chance of error if error creeps into the database.

Q569 ***Lord Morris of Aberavon:*** Is there an inherent difference between the surveillance in Mr Patel's newsagent in the morning when you or I go to get my newspaper, that being a private surveillance of a mass of individuals coming in one by one, and similar surveillance, a mass surveillance, which I have seen in the Chief Constable's office in Carmarthen of what happens on a Saturday night in Carmarthen? Are they not the same?
Dr Williams: At one level, they are the same. In a linguistic or perhaps conceptual sense they are the same, but when the state watches you, when the state's eye is above you, there is not an equal power relationship between yourself and the state. In Mr Patel's corner shop you can see Mr Patel across the counter and it is him watching you effectively by other means but when the state watches, you do not necessarily know when you are being watched; you do not know what will happen to that data; and of course the state has powers well in excess of those provided to an individual. I do believe that when there is that power in balance, and it is a matter of degree, perhaps there need to be additional safeguards directed towards the state rather than towards perhaps the small shopkeeper engaged in low-scale surveillance. It is perhaps the nature of the watcher which determines the difference.

Q570 ***Lord Morris of Aberavon:*** If there was a prosecution, the state can bespeak copies from Mr Patel's shop and I have seen it done where that very script is produced in court successfully.
Dr Williams: Yes, it can and of course in that situation a reason has arisen for the use and access of that data. There is a legal procedure for obtaining that data and there is a justification for using it on a one-off occasion. The state does not go to Mr Patel and say every day of the week, "Please copy me your tapes".

Q571 ***Lord Morris of Aberavon:*** After the disasters at King's Cross Station and the subsequent bombings, the police spent hours and hours checking everyone

who went through the station between 9 and 10 in the morning, including my own wife as it happened.
Dr Williams: I say that is simply a bigger example of the same phenomenon, though. That is a specific event that justifies access to that data *post hoc*, but the state does not routinely go to Mr Patel, or to anywhere else, and simply obtain a feed of that data on an indiscriminate basis for its own purposes; there has to be a justification before it can access that data, and that process of course does not apply where it is the state that is watching a public place.

Q572 ***Lord Rowlands:*** You refer in your written evidence to the change in technologies and CCTV for example. Would you therefore make a distinction that the rather old-fashioned set of CCTV cameras we have around the place and that has grown up haphazardly constitutes at present the same sort of dangers that you anticipate would be occurring with the new technology or can we say that that generation of cameras did not in fact infringe our privacy that much and often were properly demanded?
Dr Williams: Of course we have had CCTV for a very long time. The early cameras were very poor. I am not sure how many of the old type of technology cameras would really be around today. Certainly the City of London would be replete with fairly high-tech data processing facilities. Again, it is really a continuum but where images are recorded in digital format of sufficient quality that they can be processed, cross-matched and perhaps multiple views taken of an individual so that the three–dimensional model of that person can then be created for identity matching, that is an order of magnitude away from the old-fashioned film cameras and the grainy, 525-line, black and white technology. It is on the same spectrum but it is an order of magnitude and at some point, one that is difficult to define, perhaps we have gone beyond mere television to what amounts to data collection and that can then be fed into databases. It is not clear exactly where we have crossed that point but I do feel we have crossed that point.

Q573 ***Lord Rowlands:*** Do you feel that actually we have crossed it?
Dr Williams: I think we have, yes.

Q574 ***Lord Rowlands:*** And therefore, compared to the first generation of cameras when nobody seemed to need any authority to establish them, you really now think there ought to be some kind of specific authority to do so?
Dr Williams: I do because they are so much more powerful. They provide data of such quality and of course with cross-linking of state databases and the greater degree of information flow between different countries and different jurisdictions we now having using electronic means, the scope for abuse or the scope for excessive use, which is a kind of abuse I suppose, is that much greater. Clearly, there is a great deal of international data processing I am sure going on that would not have been the case before. We might have had Interpol wiring photographs of wanted people around the world based on CCTV at the time, perhaps in the Fifties and Sixties, but one would not have had the instantaneous exchange of data and the cross-matching of data to databases cross-linked to phone call records and trees of interconnecting people making phone calls to one another. I think the way the United States has moved in this regard rather reflects the change in capacity of technology and of course their Total Information Awareness Program, which I think has now been re-named and broken up into different departments but it is essentially the same programme, was all about and is all about the cross-linkage of those high-tech forms of information gathering with the objective of being as near as possible totally aware of the information internationally and from the US's point of view nationally as well. That includes of course presumably our own data to the extent that we would share it with them. The scope for abuse, for excessive use and, in the wrong hands, oppression if data fell into the hands of criminals or other organised groups is an order of magnitude greater and I think we have crossed that threshold.

Q575 ***Viscount Bledisloe:*** In answer to Lord Morris you said that the state did not regularly look at Mr Patel's CCTV and films, but there is nothing to stop them doing so if Mr Patel chooses to give those to the state, is there?
Dr Williams: Mr Patel would be governed by the Data Protection Act and he would have to consider requests in accordance with proportionality and so on. He could be ordered to disclose but it would be a court regulated process if he refused.

Q576 ***Viscount Bledisloe:*** He could not just let the state have them because they say they would rather like to see them?
Dr Williams: In practice of course he might. If the state made regular requests, he might not have the means to oppose that, but strictly in accordance with the Data Protection Act and the CCTV Code of Practice, one would expect him to exercise his own judgment and if appropriate refuse and then be forced, and then the police would presumably have to justify their request by legal means. The police of course do not have direct links to Mr Patel's shop, so that his eyes are not the state's eyes. There is at least that current barrier.

Q577 ***Baroness O'Cathain:*** My question relates again to Mr Patel from the other side. Is there enough protection to stop the police willy-nilly demanding

from Mr Patel that he should turn over the films from his CCTV camera?
Dr Williams: Inasmuch as if he refused, they would have to follow a legal process, there is protection, but of course there is an imbalance of power between any small individual and the state. It would be difficult to say whether there is adequate protection without really knowing the reality or not on the street as to what people in that actual position feel day to day. They may very well be very grateful for the police involvement because they probably get a lot of abuse and they would be more than willing to hand over their CCTV. It is when it is misused that the problem arises.

Q578 ***Baroness O'Cathain:*** I can understand that but it might not be just for Mr Patel. There might be somebody in the police with a grudge against Mr Singh at the next newsagents shop or whatever. Do you feel that the controls which operate on the police are sufficiently strong to avoid the indiscriminate abuse of power, so to speak?
Dr Williams: Inasmuch as they would have to obtain a warrant, that would be a protection. I really cannot comment on whether it is adequate. I do not think I have enough knowledge to answer that because I am not experienced on the ground in terms of that.

Q579 ***Lord Peston:*** I do not want to delay us, but I take it that in order to follow your question at all we need a legal definition of public space. I do not know whether there is one. I was a bit worried about Lord Morris on the railway station. The railway station is a private space; it belongs to the railways.
Dr Williams: I do not think there is a legal definition of public space but, on the other hand, one could readily formulate one in terms of any space to which the public have free or reasonably unfettered access; in other words, licensees in a private space like a railway station where the doors are thrown open to the public and, subject to certain limits, they are free to come and go. That is essentially a public space.

Q580 ***Lord Peston:*** Let us assume we know that they are all public spaces. The next question is: why would the state do this? Take the King's Cross setting; let us assume that the state decided to survey everybody going in and out of King's Cross Station. This would cost an enormous amount of money. Since your analogy with the specific angling operation with a rod and line for an individual, it is everybody, it then costs an enormous amount of money to process this and day after day it is going to come up with a lot of useless data. As an economist, I know all there is to know about coming up with useless data. I can see the worry philosophically, but I am not yet persuaded that we are talking about a real problem. It is not like in the old days the paparazzi sitting outside The Ivy and photographing everybody going in and out and occasionally they picked up a good picture. Why would the state actually do it? I can imagine other states doing it. The sheer cost of it is massive. You have to have somebody sitting there all day looking at this stuff.
Dr Williams: I think with modern technology there are two aspects to this. Firstly, the cost is not that great because of course these images and so on are automatically processed. You would not have an individual operator processing individual pictures. One would simply have large-scale computers processing the data in vast quantities.

Q581 ***Lord Peston:*** Against what?
Dr Williams: Against existing databases.

Q582 ***Lord Peston:*** So they would have to have vast numbers of pictures of other people?
Dr Williams: Such as would be gathered as part of an identity card scheme.

Q583 ***Lord Peston:*** I did not realise we were on to that yet.
Dr Williams: If I have an ID card and I have been biometrically photographed, by which I mean for example two photographs taken from slightly different angles to build up a three dimensional image, as I walk through the City of London I can be matched in a couple of seconds by CCTV and computer without human involvement. I originally qualified in visual science; my doctorate is in human vision and computer vision. There is a principle in visual science and neuroscience generally of constraint satisfaction, which is that where you have multiple noisy data sources, by combining them you reduce the noise. If you have a lot of information, you can get a very precise answer, even though the quality of your data from each individual source might be rather poor. If I have a grainy image of someone walking down the street but I watch them for a minute or two, by computational means one can resolve that into quite an accurate picture, particularly if they are carrying a mobile phone and I have the mobile phone signal; I know what their phone number is and so on. One can cross-match the databases in that way and very quickly come up with an answer, particularly if there is data sharing between jurisdictions. With international travel, for example, jurisdictions share a lot of data for obvious reasons. The American Total Information Awareness Program, as it was called, as I understand it was really all about sharing those multiple sources of data with a view to the laudable aim of getting the right answer rather than the wrong answer and getting it quickly and not ending up with junk data, if I can put it that way.

Q584 ***Lord Morris of Aberavon:*** Dr Williams, there are at least three Articles in the Convention that could affect surveillance in public places: Article 8, respect for private and family life; Article 10, freedom of expression; and Article 11, freedom of assembly and association. How has the jurisprudence developed as regards surveillance in public places from each of these parts of the covenant? What is the way forward? Do they add to or diminish the individual's rights?
Dr Williams: I refer to *Peck* v *UK* in my written submission in relation Article 8. That essentially concluded, and of course this has been departed from in the case of *Murray* now, that the mere observation of an individual by CCTV in a public place was not necessarily an infringement of Article 8 *per se*. Article 8 jurisprudence has largely focused on what might be described as individual data—privacy. For Articles 10 and 11 there really is not a lot of jurisprudence in terms of what I described as the chilling effect. I think I referred in my evidence to a couple of cases. In particular, there was one case where it was held that the gathering by general surveillance of information (by which I mean things like newspaper clippings and perhaps public photographs and so on) can amount to an infringement of one's rights of freedom of expression and freedom of assembly, but it is an underdeveloped area of European jurisprudence, if I can put it that way.

Q585 ***Lord Morris of Aberavon:*** On the jurisprudence so far on Article 8, from what you have been saying, that would stop Mr Patel and the successor to the old Welsh dairyman in London from flogging pictures of the model Naomi Campbell to *Hello* magazine.
Dr Williams: If she came into his shop, it might well not, subject to the decision in *Murray*. Of course that did not apply expressly to famous adults; it only applies to children. At present, it probably would not stop him from doing that, no. She is appearing in a public place. It is not that it is a long-lens camera taken over the wall into the garden, which would probably do.

Q586 ***Lord Morris of Aberavon:*** He is in a shop. He is not in a public place, is he?
Dr Williams: We are at that boundary between what is the reasonable extent of expectation of privacy in a shop. It would be somewhere between that of the town square and one's garden. She would have to go to court and have that litigated as to what the boundaries of her expectations of privacy would be. I do not think that has been litigated. *Murray* is obviously taking the point *vis-à-vis* an infant.

Q587 ***Lord Morris of Aberavon:*** Is that why we await developments in jurisprudence to see how far it goes?
Dr Williams: Or moves by Parliament to lay down principles. It may be better for Parliament to do that because these matters are matters of subjectivity. They are about how society wishes to be, how watched society wishes to be, and there is not a right answer as such.

Q588 ***Lord Lyell of Markyate:*** You have just mentioned the expression "reasonable expectation of privacy" and of course the converse is "reasonable acceptance of lack of privacy". The question arises that you reasonably expect a certain amount of privacy in that you do not mind going into Mr Patel's shop and he can certainly carry out surveillance on you to see whether you are a shoplifter, but if you are Amy Winehouse and you have filled your basket with very large numbers of bottles of alcohol, can he sell those photographs to the newspaper? That is a private matter that could be dealt with by the courts and the courts obviously are lurking around and it is pretty random as to what they come up with, who has got the money and where they would want to go. We are here in Parliament trying to think out sensible principles. How would you define "reasonable expectation of privacy" or illustrate it? When you get beyond that, can you give a few examples of the kinds of things which should be prevented by law or only permitted under restricted circumstances where it is carefully recorded, like for example surveillance for anti-spying purposes?
Dr Williams: Reasonable expectation of privacy: it is really for society to define that because I am sure we all have our own views. It would be circumstance dependent and it would also be activity dependent. If I am in the town square and I am engaging in political debate, I would expect to be seen by those present; I would not necessarily expect the state to be filming me and recording that, but then again I do not want privacy in the interpersonal sense in that setting. If I am simply walking through the town square going shopping, I would expect a level of privacy commensurate with the interpersonal interaction and the fact that the person near me can see me and I can go into a shop and go shopping but not perhaps that there would be a wide degree of surveillance. It is really circumstance dependent. I do not think there can be a legal definition based on derived legal principles. I think one has to sit down and decide axiomatically where one would draw that line or what kind of society are we and what degree of surveillance do we, as this society, wish to have. Different societies can choose different levels. There is no right answer, only the answer that the people define in that sense.

Q589 ***Lord Lyell of Markyate:*** But once you have crossed the line, what do you then do?

Dr Williams: One clear example of an abuse would be the example of the CCTV being used and sold for personal gain. One would want licensing of CCTV perhaps, even in a small shop like that, and any misuse by way of sale or for personal gain perhaps would be made straight-forwardly illegal rather than resting on the boundaries of data protection and the means of an individual to litigate. One could make it an offence perhaps.

Q590 ***Lord Lyell of Markyate:*** What about, for example, a parabolic camera or something going with the CCTV and showing that I am saying, or one of the rest of us is saying, that David Cameron or Gordon Brown is really for the chop, or something of that sort, which might be embarrassing if it came out? Are they entitled to do that and then publish it? Would that be beyond the pale and if so why?
Dr Williams: If one is talking about a state body, such as a local authority, doing that, then of course there would be the Regulation of Investigatory Powers Act; that would be a species of directed surveillance because it would be picking up private information about a specific individual rather than generally and there would be an internal process of authorisation, a lot of form filling essentially, internal to the local authority, before that exercise could be carried out. That evidence might then be inadmissible in court proceedings if the judge ruled it inadmissible. As an Act, the Regulation of Investigatory Powers Act is rather bureaucratic and it involves a lot of form filling perhaps rather than the degree of clarity that might be better.

Q591 ***Lord Lyell of Markyate:*** The front page of *The Sun*, is that inadmissible?
Dr Williams: There would be presumably an action in damages of some description. It is potentially against whatever individual leaked those pictures from the local authority, which would be a breach of some duty of confidence, I would have thought in that setting.

Q592 ***Lord Rowlands:*** Reading your evidence, I think you are a fan of Privacy Impact Assessments (PIAs) generally speaking. Some members of the committee have been to Canada and the United States and looked at the processes there. Could you elaborate on what you think impresses you about PIAs and also what factual limitations there are on them?
Dr Williams: I think mental discipline is important. I think PIAs, properly done, can impose that degree of mental discipline in analysing the potential impact of the surveillance programme. It requires the proposal to be broken down and considered analytically and made public. I think those are all valuable aspects. It also lays bare the internal workings of the scheme so that then whatever regulatory regime is in place can bite into those stages. For example, one could plug a privacy impact assessment into the planning system, for the sake of argument. It provides a principled way of linking regulation with analysis. That, if you like, is the good side. The bad side is that, a little like the Regulation of Investigatory Powers Act, it could resolve down to a paper exercise. I have here a copy of the FBI Privacy Impact Assessment for the DNA index database that they have. I think it runs to 1,000 words. For such a massive project, it is very worthy and it ticks all the boxes and it complies with all the criteria—a, b, c, d, e, f, down the page—but one is left with a feeling that so what, in a sense, when looking at that. I am not so much a fan of PIA; I am cautious about it because there is a tendency when one introduces schemes like that for it to end up bureaucratic, but it might provide a framework for incorporating notions of how mass surveillance might affect society as well as simply data protection issues for the individual.

Q593 ***Lord Rowlands:*** We came across in the United States in particular the concept of chief privacy officers, people installed in the organisation whose job it is to monitor and to survey all around them and to protect the privacy issue. Have you any knowledge or experience of this?
Dr Williams: Not of that directly but under the Regulation of Investigatory Powers Act local authorities will have individual people who are appointed for the purposes of that Act whose job it is to oversee the internal permission clearance and record-keeping activities and so on. That is pretty closely aligned to that sort of American-style officer, and certainly one would anticipate that in large organisations and public bodies one would want accredited individuals who would carry out a review of proposed impact assessments, reviews of those in day-to-day operations, but one would still probably want oversight by an independent body that has real teeth, because otherwise one simply has an internal authorisation programme that does not really see the light of day.

Q594 ***Lord Rowlands:*** Would you want to put PIAs on a statutory basis or would you prefer them to remain voluntary?
Dr Williams: At the moment as I have said they are voluntary. I would prefer to see them on a mandatory statutory basis. We have so many voluntary codes for very many things, but, at the end of the day, it is very difficult for civil rights to have teeth if they cannot be enforced. You do need law, I think, rather than guidance if you are talking about something as important as extensive surveillance of the population in general.

Q595 ***Viscount Bledisloe:*** In paragraph 5 of your paper you list a number, and I am not sure whether they are cumulative or alternative, of definitions of PIAs but they are all what I call balancing exercises of the desirability against the invasion. They do not deal with the legality, whereas, as you set out in paragraph 6, the first requirement in America of a PIA is to assure the handling conforms to applicable legal, and so on, requirements. Should not every PIA in this country also start by saying, "Is it legal?"
Dr Williams: Yes, and since this was written the Information Commissioner has published a handbook on privacy impact assessments at the end of last year or the start of this year. I believe a component of that is that he recommends audit as part of the PIA with respect to whether it complies with the law. These quotations, which form a gathered collection of quotations from the Lord Chancellor's analysis of responses to consultation on PIA, are not precise. They really illustrate in a sense the scope for vagueness, because it is a number of balancing exercises. There is a lot of principle involved there. Of course as part of that one has to try to tie that down. I think the PIA handbook goes reasonably far towards that in that it is clear about assessing legality, but it is an entirely optional framework. PIA does not have to happen in this country.

Q596 ***Viscount Bledisloe:*** It just bothered me that PIA might rush straight to the question of "is it on the whole a good thing or a bad thing?" and not start with "is it legal?"
Dr Williams: Part of the difficulty of course in this area is the balancing act: is it proportionate, is it on the whole a good thing or a bad thing, and so on. That may determine the legality of it. One thing that I have advocated in my evidence is that perhaps we should consider turning matters on their head and starting with a legal presumption against surveillance, so that you then have to justify. You do not simply say, "Well, we are doing it and we justify it".

Q597 ***Lord Peston:*** I am still trying to understand what the nature of the problem is, so can I just go over this again? Let me give you a practical example, and I speak as someone who is a member of the Joint Committee on Security in this building. Supposing Parliament decided that Parliament Square, which is a public space I would take it in your definition, was going to have a series of cameras around it, plus parabolic microphones, and would also take every single car number going by Parliament. Would that come within the area that you are concerned about or would you say that that is the most sensible thing Parliament could do as a way of adding to the security of this building? That is the kind of practical case that would have to arise.
Dr Williams: I am sure that is probably the position in Parliament Square now.
Lord Peston: No, we do not. What is interesting is that, unlike the City of London, and I regard this as ludicrous, we do not take every number plate going by as far as I understand.
Viscount Bledisloe: How do you know?
Baroness O'Cathain: There is a congestion charge for Parliament Square, so it takes every single number of every single car.
Lord Peston: We do not do it. I do know it. We do not even have cameras in this building, let me tell you
Baroness O'Cathain: The police do it. They are available.

Q598 ***Lord Peston:*** Let us not argue whether we should do it or not. What I want to know is this. In terms of those of us again as parliamentarians who are totally devoted to the freedom of the people of this country, would that be an example of a problem or would that be an example not of a problem?
Dr Williams: Let us suppose Parliament Square had no cameras on day one. Shall we put cameras and surveillance into that space? I would start with the presumption: no, that I should be entitled to go to Parliament without people knowing I am. Then one would have to move to whether that is justified in the particular circumstances of Parliament Square. Of course it might be because of the security situation or for other reasons. The extent to which surveillance might be justified would then need to be looked into. So, yes, it does fall within the category of case that concerns me, particularly in something as constitutionally important as Parliament Square where I may wish to assemble with others to protest or to express political views and may not wish to be watched doing that, or at least not watched without knowing who is watching me. In the United States one occasionally sees notices in public parks and other places stating that the location is a constitutionally-protected place for the purposes of free speech. I do not know what legal effect that has because I thought all Americans had a right of free speech irrespective, but one does from time to time see these signs. I do not know if they are simply there as a reminder or if they provide any enhanced protection, but one would expect somewhere like Parliament Square to be such an enhanced space.

Q599 ***Lord Peston:*** I did not know about what happens in America, which I find very interesting. You are suggesting as a minimum if we were doing anything, we ought to have a notice saying, "This is a constitutionally-protected space"?

Dr Williams: I know not whether it is merely a reminder or provides any additional rights, but at the moment of course to gather to express any view that might be construed as a protest does require a police licence.

Q600 ***Lord Woolf:*** First, may I make a general point. One of the advantages of the PIA system is that it does at least make people conscious of the need to decide whether there is any justification. That starts off favourably, does it?
Dr Williams: Yes. I think intellectual rigour and discipline is important and a framework of PIA can impose that discipline. It prevents the exercise from resolving into a weighing up, "feels acceptable all round" sort of exercise; it does indeed structure it and indeed can lay it bare to scrutiny. It is opened up in the courts. If a decision is plainly unreasonable and unsupported by evidence, it will at least be laid bare in the documentation.

Q601 ***Lord Woolf:*** That takes me on to what I really wanted to focus on. If the information that is collected is going to be used for any purpose, and presumably it must be going to be used for some purpose or it should not be there, who should be, so far as public space is concerned, responsible for reviewing it or approving it in our set-up? Is this another power for the Home Office or the Ministry of Justice?
Dr Williams: I see two different aspects. Review, on the one hand, I would perceive as effectively an internal matter to be carried out by an approved officer of a local authority or someone who is accredited or trained, but approval and regulation I would then take out of that rule and I would say someone of the standing of the Information Commissioner or an independent body of that sort ought to be responsible for licensing or indeed to have the powers to stop projects going ahead, to intervene in planning permission and effectively quash planning permission if a scheme was found to be excessive or disproportionate. I would have an independent body, not a government department. I have stopped short of saying regulation by the courts. That could come in more readily perhaps if we had a written constitution that laid down explicit rights or indeed a statute that laid out explicit rights to a presumption against surveillance. In the first instance, I would say in independent body such as the Information Commissioner.

Q602 ***Lord Rowlands:*** The Information Commissioner would have the right to receive all applications by a local authority or any organisation to put new cameras into a public space and review them and then either authorise them or not?
Dr Williams: One would have to have some sort of proportional criterion to prevent the ICO being overwhelmed but, subject to that, from my own point of view I would say: yes, the ICO should have the power to quash a public surveillance scheme if not approved by the ICO.

Q603 ***Lord Rowlands:*** That is a huge extension of his responsibilities?
Dr Williams: It would be, yes.

Q604 ***Lord Rowlands:*** It would cut across the powers of planning authorities, et cetera?
Dr Williams: Yes. I think it should be part of a profound consideration of the relationship between the citizen and the state, of which this is simply part. It may well be that a significant shift in those powers is necessary. At the moment certainly nobody would appear to have the power to quash the planning permission. There would not appear to be an overarching framework of control over mass, non-specific surveillance. So one would have to consider whether that is necessary. We do have a lot more surveillance perhaps than other jurisdictions now. Perhaps we have reached a point where that level of surveillance needs to be met with a commensurate level of regulation.

Q605 ***Chairman:*** Dr Williams, you have covered an immense amount of ground, for which many thanks. You have covered partly what I am about to ask but perhaps you could give us a final formulation of your view in answer to this. You suggest in your written evidence that if PIAs are to be successfully applied to surveillance Parliament must, and I quote, "develop a clear set of principles to be applied to assessing the social impact, rather than merely the personal data privacy impact, of public surveillance". How do you think Parliament might undertake that task? Do you think that the principles should be included in any legislation making PIAs a mandatory requirement? Do you think that the development of these principles is only a matter for Parliament and not also for the Information Commissioner or civil society groups?
Dr Williams: I think in the limit ultimately of course it has to be a matter for Parliament if laws are going to be enacted to regulate schemes of surveillance. In terms of where society draws the line in terms of how much we wish to be watched, it is a matter for the people at large, but of course Parliament is the voice of the people. One can only recommend a wide-ranging consultation with those groups that are affected. We do not have another process, short of revolution. Usually these countries that have developed massive constitutional change have undergone some very significant upheaval, but the way we do things here is by way of consideration and

consultation. We do not have anything better than that. It is certainly not a matter simply for internal political debate. I think it should be a very wide-ranging gathering of views and representation from all interested groups.

Q606 ***Lord Rowlands:*** One question that has not been listed, and if you do not feel you can answer it please say, so is this. When we were in Canada we had a very vocal case made to us that there should be a division of responsibility between freedom of information and privacy. In Canada there is a division between them; they are separate because they see the potential conflict of interest. Do you think that is a valid case and that we should have a Freedom of Information Office and a privacy officer or a privacy commissioner?
Dr Williams: I do not think it necessarily follows. Freedom of information can be constrained legislatively to cover or to exclude information about private individuals. So that if one had a sufficiently clear legislative framework, I would not be so concerned about the necessity for separation of those powers, but it may well be, and I think it probably is, the case that in Canada they have a more wide-ranging freedom of information right perhaps than we have here. I do not know personally. If they have more wide-ranging freedom of information rights, then one can readily understand that there might be a conflict between those two. If one can formulate legislation that does not place the two in conflict, then one does not face the need for separation.

Q607 ***Lord Rowlands:*** Do you think at the moment we have that legislation right?
Dr Williams: As I understand it, freedom of information requests would be declined if they relate to individually identifiable private data.

Q608 ***Lord Lyell of Markyate:*** You refer to developing a clear set of principles. It sounds very sensible. Have you thought about this? Have you written anything about it or if we were to ask you to write to us with two sides of A4 as to what those principles should be, would you be able to do so?
Dr Williams: I certainly would be willing to carry out that task. I have not written anything other or beyond what I have written in my submission. I wrote a longer version of that that has been published in one of the journals, for which I can give the reference. The focus I think would be on the chilling of the exercise constitutional rights and perhaps there ought to be a review of jurisprudence on that. It is much more of an international matter in the sense than it is a national matter. I can certainly produce something.
Lord Lyell of Markyate: It is really the principles: you talk about the review of jurisprudence but you and I know that that is very scattered.
Chairman: Dr Williams, you have been extremely generous with your time. May I thank you on behalf of the committee for being with us and for the evidence you have given.

Examination of Witness

Witness: Professor Ian Loader, gave evidence.

Q609 ***Chairman:*** Professor Loader, good morning. May I welcome you to the committee and thank you for coming. Perhaps, as we are being recorded, you could identify yourself for the record.
Professor Loader: I am Professor Ian Loader. I am Director of the Centre for Criminology at the University of Oxford and a Fellow of All Souls' College.

Q610 ***Chairman:*** May I begin by asking what constitutional or legal issues are engaged by using mass and individual surveillance in the pursuit of national and personal security? Is there any evidence that surveillance has a chilling effect on citizens' ability to enjoy freedom of association or expression?
Professor Loader: Can I come to that question indirectly because what one thinks about the constitutional implications of mass and individual surveillance rather depends on how one analyses the situation we are in and how we got here. It seems to me that that situation is best characterised by a circumstance where governments and security institutions increasingly pursue a certain conception of what security means—and I am happy to talk more about how I think we might otherwise think about security—which requires ever-increasing numbers of measures in order to pursue the thing that we want to achieve. The thing we want to achieve is the reduction or elimination of risk. This means, I think, that we as a society have established a certain kind of both speed and direction of travel of which the development of mass surveillance measures and/or individual target surveillance measures are but a part. This has been brought home to me because for the first time in many years I was searched under Section 44 of the Terrorism Act while waiting to come in here, but that is by the bye, because I was sat in Parliament Square of course. The sheer amount of criminal justice legislation, of new measures and new Acts and new criminal offences seem to me part of a pattern of how our society responds to threats of crime, terrorism and anti-social behaviour, of which the main practices are but a part but a significant

part. The speed, it seems to me, to have something to do with that general sense of escalation of activity and what I have elsewhere called legislative hyperactivity. By the direction, I sometimes think that surveillance measures in general, and let us take closed-circuit television cameras as an example, are what you might describe as destined to succeed. If it can be established that they have been a success in reducing levels of crime or fear of crime, then the answer is that we need more of them. If it can be established that they have not succeeded, then the answer is always that we need more of them. Indeed the Metropolitan Police said something along these lines only just last week. It seems to me that the consequence of that is that there is a ratcheting up process going on here. In other words, that once you put certain kinds of measures in place, it becomes very difficult to imagine the circumstances in which you could successfully take them away again, either legally, politically or culturally. Therefore, the direction of travel, once established, is quite difficult to halt. If one takes that as the starting point, and it is mine at any rate and I will happily say more about it, then it seems to me that there are the following constitutional implications. The obvious one is that what we are talking about here is the relationship between the individual citizen and the state. The extent, intrusiveness and measures we use to think about and control surveillance practices and anti-crime practices more generally are at the heart of that question. Secondly, in this environment we have become rather keener as a society, as a government, as a legislator—and in times of heightened uncertainty and concern about crime or anti-social behaviour or terrorism you can see why this happens—in thinking of the measures that we put in place to prevent or protect us from those threats than we do about systems of accountability, oversight, monitoring, redress and so on. There is a certain lag in our capacity to become enthusiastic about certain things and in the kinds of institutional mechanisms that we put in place in order to try to subject these anti-crime practices to certain types of control. Thirdly, it seems to me that what follows constitutionally from the analysis I have just briefly sketched is that what our society currently lacks is a series of mechanisms that enables us routinely to pause, reflect and ponder the judiciousness, wisdom or consequences of the particular kinds of measures that we are putting in place to pursue security; in other words, to pose the question: when is enough enough and do we need another round of this legislation this year of a similar kind to what we had last year? Do we need this or that power? What constitutionalism does in that context at its best is put in place precisely those mechanisms that allow us to decide how we are going decide—to pause, reflect and develop cultures and practices of justification. It seems to me at least that that is a significant part of what is at issue currently in this discussion. I am happy to pause there. I can talk about chilling if you want me to carry on.

Chairman: No. I think that you have just most recently described precisely what the functions of this committee are.

Q611 ***Baroness O'Cathain:*** Do you think it is inertia or apathy on behalf of the general public that has allowed this surveillance creep as we call it now? To follow what you have just said, do you think the public really want to pause and reflect? Is there any demand out there for anybody to put a stop to all of this, to the endless march of technology?

Professor Loader: It is a difficult question to answer. I spend a lot of my time when I am doing my research talking to people about these very questions. My best guess is that this is a minority view, if one that is sometimes very angrily and loudly propagated, that there is among a section of the population a certain amount of enthusiasm for some of these measures. They recognise that the crime or terror, or whatever it is, is a problem and it seems only reasonable that we would do anything that we possibly can about this. I am not sure that that level of enthusiasm is widespread. The more general reaction to these things is either not to think about them very much at all on a day-to-day basis unless prompted to do so or to be indifferent or to have a series of quiet grumbles that one does not really know how to translate into anything that you might call activity. The question about the chilling effect was posed in your written submission to me. I thought about this. My initial answer to the question "is there any evidence of a chilling effect" is that I do not know whether there is. Then I was led to think about what would count as good evidence of a chilling effect having taken place. One aspect of that might simply be that level of public indifference and apathy. It is a cause of some puzzlement to me why we have gone, for the sake of an example, in a very short space of time, say 20 years, from having very few surveillance cameras in public spaces to having many more than any other country on the planet without, it seems to me, any kind of serious public discussion about whether either this is a good idea on ethical or political grounds, or even whether this is a good use of what remain scarce public resources to be devoted to questions of crime prevention and crime control. That remains something of a puzzle to me. It may be that if there is a chilling effect, how we measure it is down to a certain degree of fatalism. These things are just going to happen; I might not particularly like it or dislike it or think much about it but what can I do? If I do not want a CCTV camera in my town centre or here or there, what exactly do I do? Do I write to my MP, do I write to this committee, do I join Liberty

or do I just do nothing? I rather wonder whether if you wanted a single encapsulation of where we are, it might be something rather more akin to that. Another thing that puzzles me in this context is why ID cards seem to be building up a head of steam of overt and organised opposition and disquiet. There may be all sort of cultural reasons to do with the English and ID cards that are at play here. It may be that they have just become something tangible. In the context where there is a level of unease and disquiet about the way things are going and you do not know how to get a handle on that, ID cards may present themselves to people as being something that they can grasp and dislike and draw a line in the sand. I cannot back that up. That is hypothesis.

Q612 ***Baroness O'Cathain:*** Getting back to surveillance, the justification for surveillance is usually stated in terms of national or personal security. What role do you think legally enforceable human rights can or should play in setting limits on surveillance activities, or indeed what does the general public know about legally enforceable human rights?
Professor Loader: The answer to that question I rather suspect is: not very much. That may have some bearing on how we think about the best possible answer to the first of your questions. You could take the view that human rights are legally enforceable protections and we when want to think about the best ways in which we put in place legally enforceable protections, we just think about lawyers and what they do. It seems to me that we also have to give some thought to the question of the ways in which any kinds of right to protection has some wider purchase on public opinion and sentiment. I am not sure that human rights protections in this field, or indeed even the question of how one goes about establishing a more robust regulatory regime for surveillance practices in general, CCTV systems, press themselves very heavily on public or political consciousness right now. I have no easy answer to what you might do about that.

Q613 ***Viscount Bledisloe:*** Before I put my question, can I make one point plain? Amongst the various suggestions you made was that people who did not like it should write to the committee. That is a very, very bad idea! Is not a main factor in what you were talking about the fact that people just do not know what is done? I suppose I reckon I know a bit more than most people but until I sat on this committee, I had no idea that if I pay for my Oyster card with my credit card, all my journeys are then logged against me. There are thousands of other things. I did not know there were CCTV cameras that could bug what you said. Ought not there to be some way in which there was more public knowledge of what actually is happening?
Professor Loader: I am not sure what one would do with the information. I too only discovered a couple of weeks ago that if you use an Oyster card your journeys through London could be tracked by London Underground.

Q614 ***Viscount Bledisloe:*** For example, I pay for my Oyster card with cash.
Professor Loader: There are other examples. As we know, if you use a mobile phone, you are leaving a permanent trace of your movements that the authorities could, if they so wish, retrospectively recover. The same happens when you use a cash point machine and with supermarket loyalty cards; supermarkets can use that information to generate all kinds of information about your consumption patterns and your lifestyles, which they could then use as they see fit. Many of those things seem so embedded in contemporary lifestyles, what can you do? Your only option in the mobile phone instance is not to have a mobile phone. Most people think not having a mobile of phone is to reduce the quality of your life, not enhance it. That may not be true. The point I am making is that if one feels a level of disquiet about many of the ways in which you are surveilled as you go about your routine business as a law-abiding citizen, there is not much you can do about it on a practical level.

Q615 ***Viscount Bledisloe:*** For example, supposing everyone knew that if they use their credit card, it is all logged and shared around and everything: would there not be a large market for a credit card that undertook not to do that?
Professor Loader: I do not know. The thought that goes through my mind is: if that is true, why has no-one taken advantage of this market opportunity just yet?

Q616 ***Lord Rowlands:*** You said in your earlier remarks that there had been a stream of criminal legislation and that we need to pause and ask what the effect is. There is a growing method of doing that apparently, which we call post-legislative scrutiny. Of all these Bills that you refer to, the stream of Bills that have promoted surveillance, which ones do you think we should target in post-legislative scrutiny?
Professor Loader: That is difficult, just sitting here, without looking at them in detail.

Q617 ***Lord Rowlands:*** There has been a whole stream of them.
Professor Loader: I think the problem is that if you took any one of those Bills one by one, you might, as the Government has been minded to do, come up with several plausible reasons why this particular Bill

was required to deal with this particular problem. When you look back over 10 years of legislative activity, you suddenly discover—and I discovered this to my shock and surprise—that there have been more pieces of criminal justice legislation in the last 10 years than there were passed in the previous 100. I take a lot of persuading that we live in such dangerous times that we require such a step change in the amount of legislative activity that is devoted to questions of making us individually and collectively safer. The problem, as I see it, becomes apparent when you look at the pattern in aggregate terms; it does not necessarily mean you go through the 66 and say that we can filter out these 10 and we really did not need that one or that one. The problem we are confronted with is why is it? To me it is a genuine puzzle and it will be a puzzle for future historians I think: why is it that this Government has become just so busy in the field of crime, criminal justice and punishment. There are all kinds of reasons that we could talk about, but nonetheless it seems to me irrefutable that it has become extremely busy. It is not obvious to me that our society is either safer or a better place to live, considered in the round, as a consequence of all that activity.

Q618 ***Lord Rowlands:*** Presumably, and governments do not do it willy-nilly, in many ways this would be being reactive or responding to situations or responding to sentiments that parliamentarians and politicians are picking up from the public: yes, we want anti-social behaviour orders because there is a bunch of young yobs who have been causing mayhem in the square or in the street. This is how it arises.
Professor Loader: That is undoubtedly what they would say. There is undoubtedly something in that in that it is impossible to work out whether your method of detection is your postbag as an MP or your reading of the papers or just what you hear in the ether about a level of public concern and alarm as to certain kinds of problems and places that properly require democratic government to respond. Whether that unproblematically translates into 66 pieces of criminal justice legislation and everything that has gone in train with that seems to me to be a rather more open question, shall we say.

Q619 ***Lord Rowlands:*** You cannot identify say three or four Bills or Acts that in retrospect we should re-visit in post-legislative scrutiny?
Professor Loader: If you gave me a bit of time, I would be able to do that. I do not think I can do that just sitting here now with any confidence.

Q620 ***Lord Rowlands:*** Could you send us written evidence to that effect?
Professor Loader: I could look at that.

Q621 ***Lord Woolf:*** I have just two points, and I want to see whether you agree with them. You point out that with this legislation, treated individually, you can always see some form of justification for it, one hopes, but what has been lost sight of is that the sheer volume of the legislation has very damaging effects on the efficiency of those forces which should be achieving what the legislation is designed to achieve if the object is to reduce crime. For example, the judges have been ignored; they have been crying out for years, saying "Please, leave off this legislation, because we just cannot deal with it. The educational efforts that are required are so very considerable." That falls on deaf ears because of the political will to do something which appears to the public to be beneficial but is not beneficial for the reasons I have just indicated. You cannot just look at the legislation. You have to look and see the consequence of magistrates having yet another thing to learn, and the consequences of judges having to spend more and more time on it. I wanted to put another aspect of that before you respond. Are we not getting to a situation where perhaps the obvious disadvantage of intrusion on the individual's right to privacy is self-correcting, because so much information has now been collected that, even with the vast sophistication of dealing with information, really, we cannot keep up with it, in the sense that the expense of finding out what the information could provide is so great that it can only be used for limited purposes?
Professor Loader: Let me take each of those things in turn. I think your analysis of what has happened is broadly right. One of the explanations for the step change in Government activity I think is because—and this was rather more pronounced under our previous leader than our current one, at least at the level of public rhetoric—they saw themselves as the consumer's champion, taking on the forces of remote bureaucrats who ran, in this case, the criminal justice system, and that included judges, that included police officers. They therefore saw as their job to make sure that that system bent, as far as it could be made to bend, to the Government's interpretation of the public will, and the public will was that they wanted more things done about crime and whatever. That has also had consequences for the capacity of that system to cope with that sheer level of initiative and new pieces of legislation, and so on and so forth, which may mean that on the ground things have not played out in the way the Government might have intended. CCTV might be a good example of that. It is sometimes said that inefficiency is a great check on the power of the state to intrude in the life of the citizen, and there is something in that. CCTV is a good example because, I suspect, and indeed, there is a certain amount of evidence to establish this, that

what mainly happens in an awful lot of cases is nothing, that only some of the systems are routinely monitored on the basis that some just record, some are dummy cameras, and that anybody who wanted to seriously use this information would just experience a massive sense of overload and an incapacity to register and do what they wanted with it. That is not to say there are not aspects of this development that are not problematic. Nonetheless—I do not know what the best phrase for this is—the barking may be louder than the effect of the biting on the ground. I cannot think of a better metaphor off the top of my head.

Q622 ***Lord Smith of Clifton:*** Professor Loader, of course, before the spate of legislation that you have talked about that we have had since 1997, prior to that, in a sort of microcosmic way, we had 30 years of experience in Northern Ireland, where there was a spate of specific legislation for Northern Ireland which by and large was neither necessary nor used in the fight against terrorism and civil disturbance. Do you agree with that? In other words, we had had a laboratory experiment in Northern Ireland before we applied it to Great Britain. Secondly, if you do do a quick look for us about the effects particular Bills have had and what, in post-legislative terms, might be recommended ditching, or at least having a look at, I wonder if you could possibly include the experience of Northern Ireland over the 30 years before 1997, because I suspect you would find much the same sort of story.
Professor Loader: I can certainly have a look. I am no expert on the experience in Northern Ireland at all, so I venture into this territory rather hesitantly. I know things I could look at to think about that question.

Q623 ***Lord Lyell of Markyate:*** We are trying to find what is acceptable in surveillance and what is beyond the pale. Can you give us, quite briefly, three examples of things which you think are broadly acceptable and three examples of things which you think are definitely beyond the pale?
Professor Loader: I think what becomes acceptable in broad terms—and this may or may not be an adequate answer to the question you pose—is targeting resources and technologies and legislation where you can identify particular kinds of problems or neighbourhoods or locations where they can be effectively used. In other words, I think the argument I am making is an argument for what you might call judiciousness or prudence, in other words, for thinking rather carefully and targeting resources in appropriate weight. What I find most objectionable about the way we as a society have embraced CCTV is the kind of rather scattergun approach that we have used to this, which a bit of me finds deeply troubling at the level of waste of money, apart from anything else, because it is just assumed that this is some kind of all-purpose solution that we can use. I think what we need to do, and what I would approve of, is careful and appropriate targeting, with appropriate forms of regulation and accountability and transparency that can give people greater levels of confidence that those systems are being used in the way that they are. What do I think is beyond the pale? I suppose the inverse of what I have just said is beyond the pale, the sheer unthinking speed with which we now put into effect surveillance and other kinds of anti-crime technologies, and the disregard that we give to the implications that they have both in how they work on the ground and for questions of liberty.

Q624 ***Lord Lyell of Markyate:*** That is a bit of a surprising answer to me, because it seems to be based entirely on questions of efficiency and not on principle. For example, would you not agree that, albeit there may be far too many CCTV cameras—I do not personally think there are but there may or may not be too many of them—they are not really doing anybody any harm? They may be wasting some money. That is quite possible but that is a different question. On the other hand, if people were using parabolic microphones to track you in your conversation up from the High towards All Souls and were then using that to hold it against you to show that you were an anarchist—which I am sure you are not—that might be regarded as beyond the pale. That is what I am referring to as matters of principle.
Professor Loader: That is a misreading of my position. My criteria for judging these things are not efficiency and effectiveness so I am sorry if I conveyed that impression. Clearly, that would be an example. I am currently involved in some research. Investigating the ways in which CCTV companies go about selling their wares is our research question, and we are in the early stages, but it seems to me that one of the things about the CCTV industry as a market currently is, one, in this country at least, the market is fairly saturated, so I have now lost track of the number of CCTV providers who say that Eastern Europe and the rest of the world is where they are headed because there is not much more you can do here, but the one thing they can do here is, when you have systems that require updating, as 20-year-old systems frequently do, they are now able to say to people, "We now have much more technologically sophisticated kit that we can sell you, and it can do things that your old system cannot do," and it can do things that are increasingly sophisticated, like logging on to individuals and following their movements, recording their movements, typing in particular kinds of profiles of individuals, and all that kind of stuff which I am sure you have come across. That seems to me to raise rather more serious intrusion on people's privacy and

liberty questions than the standard CCTV camera that simply records the mass of movements of people walking down the street and does nothing else. The sheer pace of technological change in terms of what the equipment can do raises some profound questions about our capacity, because it enables people to think about forms of crime control that were not previously open to them, and raises serious questions about our capacity to think about the ethics of them and their human rights and liberty implications.

Q625 ***Lord Peston:*** If I can start with a comment, as far as we know, politicians are now held in lower esteem than they ever have been in the history of our country, yet at the same time, given any problem, the public seems to demand that these very same politicians do something about it. That seems to me to be really paradoxical, and I think it lies behind a great deal of what you yourself are saying, namely, that "something must be done" is what is always being said. Every day. I think there was one on knives today. Because several people have tragically been killed with knives, the Governments suddenly announces I cannot remember what intensification, or maybe it is the Met has suddenly announced some intensification of knife search, but it is simply a problem and we have to do something, even though we lack all the evidence that doing anything does anything, if you know what I mean. The best example we have had in the last week is the reclassification of cannabis. Any economist will tell you what that does is raise the rate of return to all the illegal dealers. You wonder whether no-one has ever seen a film to do with the Twenties in America. Nonetheless, they suddenly decide—in this case it is a government I support—that they must *do* something, with the italics on "do"—even though any analysis tells you that this will produce the exact opposite effect. Do you have any explanation for this? I have always cynically taken the view on the legislation that full employment for lawyers is the main target for this Government. That is a cynical view. Do you not agree it is paradoxical that governments cannot say in many cases "It is terrible but there is actually nothing we know of or that we can think of to do"? Governments are not allowed to say that.
Professor Loader: I agree that is a paradox. I think the other thing you discover if you, as I do, spend your time tracking and thinking about political responses to crime and their relationships to the crime problem, is that it is strong and confident governments who feel most able to have an intelligent conversation with the public about what can and cannot be done to address and respond to crime risks, and politically weak and faltering governments find it extremely tempting to use crime as a means of shoring up their legitimacy. It always strikes me—and I risk becoming an amateur political journalist at this point, but there we are—that one of the things about the Blair government is that it was strong but unconfident; in other words, it was concerned that its majority could be blown away at a stroke, and therefore the attention on crime was, at least in part, an attempt to shore up its constituency of voters who had supported it. If you look back, in retrospect, over the 18 years of Conservative rule from 1979 to 1997, there was lots of huffing and puffing and making tough rhetorical noises but the record of that government was extremely mixed. The times at which that government most commonly resorted to what you might describe as tough law and order measures were at the beginning, when Margaret Thatcher was the most unpopular Prime Minister in recorded polling, and at the end. At the time in which Margaret Thatcher was at the peak of her political powers, we put in place under Douglas Hurd what became the Criminal Justice Act 1991, we reduced the prison population, the government engaged in a reasoned, rational and coherent dialogue about how our society responds to crime. It seems to me that the political conditions for moving away from that kind of consumerist politics that says "You, the electorate, are very worried; we, the government, our job is just to respond rather uncritically to what we think you are telling us." A government that says "There are these kinds of resource constraints, we have these kinds of trade-offs, and there are these kinds of human rights considerations to enter into the equation," a government that is able to have that informed dialogue with the electorate about how we go about thinking about and responding to crime or terrorism and anti-social behaviour requires a certain amount of political courage in a world where governments think that the loyalty that their voters have to them is rather looser and more contingent than it was, say, 30 or 40 years ago.

Q626 ***Lord Peston:*** Can I make one other observation on that so that we do not just concentrate on lawyers? It is still the case that the majority of medical conditions are such that a doctor can make no useful intervention when the patient presents, but no doctor is capable of saying "There is nothing I can do to help you," so we get vast over-prescribing of drugs simply because the doctor feels he cannot let the person walked out of the place with the message "There is nothing I can do for you". That is the exact analogy again professionally for governments and lawyers. The answer "I can do nothing to help you" is not an acceptable answer.
Professor Loader: Can I just respond to what Lord Lyell said a minute ago, at least in these terms, which is to say that one of the consequences of the ways in which we have come to think about these things is we have got into an unfortunate position of treating

liberty and security as if they exist in an almost entirely zero-sum relationship. That seems to me to be a deep mistake. It is a deep mistake for this reason. I have just written a book which is an attempt to answer the question "What does it mean for individuals to be secure?" Individuals are partly able to feel secure because they live in an objectively secure situation. In other words, they feel the levels of risk that they face are relatively low or manageable, but they also have to have some kind of secure feeling, in other words, part of security is a subjective sense of well-being, freedom from anxiety, and that does not only flow from your levels of subjective risk. It flows in part from your capacity to feel that you have some kind of confident, effortless sense of belonging to the society of which you are a part. How the government behaves in the broad span of its activities has a deep bearing on that aspect of your security. If you think about security like that, human rights protections have a significant importance not only in checking what governments can do and the kinds of powers they can afford themselves, but also in registering certain kinds of counter-majoritarian protections for those who are frequently the target of at least more specific forms of surveillance. If you start to think this through, it becomes clear, put at its most stark, that human rights are importantly a pre-condition for achieving security, or at the very least that those two terms do not exist in a relationship of deep tension in the ways that it increasingly is now presented to us.

Q627 ***Baroness O'Cathain:*** Can I come back to Lord Lyell's question and your answer to it, because he did ask for things that were acceptable and were not acceptable. Your first answer was targeting technology et cetera in "appropriate weight". Who is going to dictate what is an appropriate weight? How do you come to the conclusion what the appropriate weight is? Is there any way of measuring that appropriate weight?
Professor Loader: I am pausing as I find it hard to know, off the top of my head, what that appropriate weight would be.

Q628 ***Baroness O'Cathain:*** You said it.
Professor Loader: Yes, I know I said it.

Q629 ***Baroness O'Cathain:*** It is a difficult one. It has had me musing ever since you uttered those words.
Professor Loader: In a sense, you can pose the question at both an individual and, as it were, a policy and resource allocation level, because at an individual level you want to know. I often wonder about the Metropolitan Police operation at Forest Gate in this context. Ian Blair probably did the only thing he could do in those situations. In other words, he got intelligence that there was a terrorist cell in Forest Gate, and it takes a very brave Police Commissioner to say "I think that is dodgy intelligence. I'm going to do nothing." So he did what I think anybody in his position would do, and he acted on the intelligence he had, only subsequently to discover that that intelligence was not very good. The problem for someone like Ian Blair is that you cannot keep doing that. You cannot keep throwing up false positives without having some very serious consequences for police relationships with, in this case, the Muslim community, which is a problem not only at the level of the principle of policing by consent but at the level of effectiveness, because effective counter-terrorism policing, as Ian Blair well knows, requires people in the Muslim community to supply them with information. The more Forest Gates you have, the more difficult that process becomes. This bears on the appropriate weight question, because it does seem to me—and there was a question there about intelligence-led policing—that you need to think about the kinds of intelligence coming your way and have procedures in place for distinguishing what you call intelligence from information, gossip, hearsay and all the other things that people might say to a police officer about Bloggs who lives at number 13. That question also seems to me to emerge at a resource distribution level, because it does seem to me that you want to find some way of trying to align resources with some sense of objective risk.

Q630 ***Baroness O'Cathain:*** Do you think that is ever going to be possible, because you are trying to balance practical resources with emotional responses?
Professor Loader: I think it becomes more possible if you can summon up the confidence to try and engage in forms of rational dialogue about the problems that we face rather than seeing it as your task to jump to the tune being played by those emotional voices.

Q631 ***Lord Morris of Aberavon:*** I will ask my question in three parts because I think they are interdependent and follow on each other and are consequential. First—and this is slightly up in the air in view of recent judicial developments—do you think that a right of privacy enjoys a sufficiently solid foundation in jurisprudence in this country? Secondly, how important is a right of privacy as a safeguard against the excesses of surveillance? That begs a question in itself, and you have given an illustration of mobile phones, and we know that evidence can be produced in court of actually the time the call is made and the place, down to this room. My advice to a terrorist would be—which they do, without my advice—do not use the same mobile phone but have 200 SIM cards. That is one of the problems about the 42 days we are talking about at the moment. Thirdly, how can the current

arrangements, DPA, the Regulation of Investigatory Powers Act, information and interception and surveillance commissions, those statutory arrangements, be strengthened or supplemented?
Professor Loader: The first question you asked is the one I thought I could not answer. Many years ago I did a law degree but I no longer think of myself as being a lawyer. If you want to seek some advice on the place that privacy has in English jurisprudence, I am not your man, I am afraid, which is not to say I do not think there are some interesting questions about privacy here and what privacy now means. It seems to me that privacy must and should remain an important part of our conversation when we think about surveillance, as both a value which we wish to cling on to and a something which you might want to give legislative effect to, because the capacity to control information about your life and your doings seems to me an important part of what it means to have some kind of capsule around you as an individual and a sphere of autonomy within which to operate that the state cannot encroach upon. Of course, that just becomes much more complicated in a world of mobile phones and the Internet and global networking and so on and so forth. One wonders in this context—and I just pose this as a hypothesis and I am not the first person to do so—whether privacy means the same thing any more to people who are in their twenties than it does to someone like me in their forties or other Members in this room. In a world of social networking, where people seem very freely able and willing to give up their privacy and advertise all kinds of their doings to complete strangers, legally or socially, what does privacy any longer mean? There seems to me in that case an argument for hanging on to it. Maybe in that world a legal right to privacy becomes more important, and it becomes significant that you place firewalls between what people have freely entered into the public domain in a certain context because they are wanting to communicate with their friends, and what other people can do with that information in other spheres of their life. So if you suddenly decide to put some pictures of yourself up on a Friday night, drunk, on the streets of Oxford, 15 years later can an employer use that picture not to employ you, or can a police force use it to infer that you are a person with a disreputable history? I think that is all rather troubling. What one does to try and erect those firewalls which, as it were, give some credence to the context in which that information was first generated, I think that is a difficult challenge to which I have no easy answers but I think it is a challenge which we all need, rather pressingly, to think about. Your third question—one bit of this that has always irritated me, so I might as well get it off my chest since I am here, is this. One of the unpleasant and damaging social consequences of the advent of a surveillance society is the use of surveillance as entertainment, not least because one consequence of that has been to some extent to spread the idea that we live in a society which is falling apart, which is broken, which is violent, which is dangerous. So if I were to forbid one thing, I would forbid police forces from being able to sell CCTV footage to television companies. I think no social good can come of that practice.
Baroness O'Cathain: Would you also ban programmes like "Big Brother"? There is one in the jungle as well, is there not?

Q632 ***Chairman:*** "I'm a celebrity, get me out of here." I hasten to say I never watch it.
Professor Loader: Possibly for aesthetic reasons!

Q633 ***Baroness O'Cathain:*** This is a serious point because you do raise this issue, and the fact is, those very programmes give people the right or seem to give people the right to think that they should know every darn detail of every single individual they want to know about.
Professor Loader: Absolutely, and I think that is an important part of this conversation because, if that becomes a much more widespread public sentiment, it then becomes very difficult to argue that anybody, least of all someone as deeply unpopular as a suspected offender, should be able to keep certain aspects of their doings secret from anyone else or the authorities, which is partly why I raised the question about the changing uses and meanings of privacy in our society. I think that is a very central part of the issue that we are confronted with.

Q634 ***Lord Morris of Aberavon:*** Can I be precise as to what I was asking earlier? Are the existing pieces of statutory machinery and the organs set up sufficient to deal with fast-moving technologies, not only fast-moving but maybe much bigger investment in existing measuring technologies? Let me give you an example. You can go to quite a few shops in London and buy highly sophisticated listening devices, highly sophisticated sights which can pick you up a long way away, and there are a whole host of bugging devices which are easily available so the public. Secondly, perhaps more mundane, it was Lord MacLaurin, the former Chairman of Tesco, who said in the memorable phrase that when he engaged experts to measure the use of club cards in his shops, he knew more about the business in three months from their work than in a lifetime of working in that particular industry. Those are the kinds of development happening. Are the Acts of Parliament sufficient to deal with this, or should they?
Professor Loader: My hesitation is only because surveillance is not sufficiently my area that I confidently know what those regimes are currently. My hunch is, in response to the examples you give,

no, but that requires us to think about exactly how they are lacking. Maybe certain forms of those technologies should require a licence. One needs certain kinds of constraints on consumption. Maybe we need more robust constraints on what individuals can do. What does one do with a supermarket's customer loyalty scheme? What would be the grounds on which one might, for example, want to make them illegal?

Lord Lyell of Markyate: What one does is to invite a professor from All Souls to give you an answer!

Q635 ***Lord Rowlands:*** People volunteer. Presumably, when you take loyalty card, you are volunteering. Would you ban volunteering?

Professor Loader: Precisely. It is a consensual exchange between adults, is it not? That is why I posed the question: what grounds would you mobilise to say that shops should not be able to operate such schemes when their customers want to effectively hand over information about their consumption practices in return for slightly cheaper goods? That is what is going on.

Baroness O'Cathain: Can I just intervene here, as an ex-board director of Tesco, who was actually on the board when we decided to go down the club card route? It was done solely, in the beginning, to make sure that everything was going to be in stock. It was done on bar codes. Then they really realised it would be a good marketing tool if somebody buys an enormous amount of a certain wine occasionally to give them the opportunity to buy it at a discount. I am sure Lord MacLaurin, to be fair to him, never really meant that he knew about his customers. He probably knows the toothpaste they buy but he does not know what they do or what they work at or anything like that. We are getting confused now, far too confused. A customer is not a fool. They know exactly the reasons for loyalty cards, and I bet practically everybody around here has a loyalty card.

Q636 ***Lord Morris of Aberavon:*** My Lord Chairman, I am not arguing the merits of any of these, either for or against. All I was trying to elucidate, in which I felt earlier, was whether the present statutory bodies are sufficient to deal with developments, whether technological or whatever. That is the sole question.

Professor Loader: My honest answer would have to be that I do not know. It is not sufficiently my field, nor something I have studied in detail, to feel I can come to a Committee like this and give you an answer, so I ought not give you an answer.

Q637 ***Lord Peston:*** Preliminary to that, of course, Karl Popper pointed out to us many years ago that many apparently good things can have appalling unexpected consequences, and that includes loyalty cards and almost anything else we have ever invented. On intelligence-led policing, which you have led us into already, I take it what you mean is information-led policing as opposed to "use of your intelligence as a person" kind of policing. One of the things that troubles me is the approach to policing, which often, to me, as an outsider, seems plainly idiotic. Let us get to intelligence, by which you mean information-sourcing. You said, it seems to me overwhelmingly correctly, that you need public co-operation and public support for this kind of intelligence policing. If you go through the logic of it, what is troubling, and I think you are guiding us towards it, is that you sit there and you say, "Well, who are the likely terrorists?" That is trying to analyse it, and you think nowadays it is members of the Muslim community in our society. This is post the IRA. Therefore that is the community we have got to get information about, which is also the community we have got to get information from. Is there not really a problem there precisely in that way, that you want people to co-operate but, in a sense, they are "shopping" fellow members of their own community? Is that not the nature of the problem? That is the problem, presumably, that Ian Blair ran into.

Professor Loader: That is exactly the nature of the problem and, of course, it is a problem with a history. Police relations with the Muslim community did not suddenly start on 12 September 2001. There is a pre-history that continues to shape and structure the ways in which minority groups relate to the police. Part of the problem the Metropolitan Police has is getting over the "Why are you only interested in this community and its problems and its issues now, when we have been defined as a threat, when prior to 2001 we can mount a reasonable case to say that our interests were not very high up on the list of priorities?" There is a kind of "Johnny-come-lately" problem that the Metropolitan Police has to get over. The trick is to try and find ways—and Ian Blair will know this—of trying to establish greater forms of confidence in that community, not only in how the police treat them but in ensuring that those members of the community feel secure, i.e. feel secure in the sense of enjoying an effortless, confident sense of belonging to the society in which they live. Of course, every single police action bears on that question: every time you are stopped and questioned, how you are stopped and questioned, when you are stopped and questioned. When I was sat in Parliament Square at 11.20 and a police officer came and spoke to me under section 44, I did not feel that my secure and confident membership of this society was at stake in that encounter. I might not have wanted the encounter to happen but I did not feel it was at stake. If I were a 15-year-old Muslim having that encounter, I think I would be more minded to feel that my confident, effortless membership of this society was at stake in that encounter and I had better

behave in certain kinds of ways. The trick is to try and find—and this is not only a police problem—all kinds of strategies and policies that make the Muslim community as a whole feel that they belong here, and not that they are just a threat, who only come to our interest and concern because we want them to shop the members of their community we think may be extremists.

Q638 ***Lord Peston:*** In a sense, it really is a matter of making sure—which is not really for the police, it seems to me—that they feel like members of our community. I have certainly been stopped and searched once when I was much younger, going to a football match, and I thought it was marvellous that I had been singled out as the most likely dangerous person. I felt very much a part of society, one of the boys! I might add that I was stopped by a lady policeman, which made it even better. I think with some parts of our community the problem surely starts earlier than the police. It is to do with the fact that they do not feel part of our community anyway, which I take it is what you are saying.

Professor Loader: Yes, absolutely. Like any other crime problem, there cannot only be a policing solution to it.

Chairman: Professor Loader, you have been extremely generous with your time. Thank you. I think we have guessed the title of your new book—it is going to be called "The era of Buggins' turn"! Thank you very much indeed for joining the Committee, and for the evidence you have given.

WEDNESDAY 21 MAY 2008

Present
Bledisloe, V
Goodlad, L (Chairman)
Lyell of Markyate, L
Morris of Aberavon, L
Norton of Louth, L
O'Cathain, B
Peston, L
Quin, B
Rodgers of Quarry Bank, L
Rowlands, L
Smith of Clifton, L

Examination of Witness

Witness: Sir Christopher Rose, Chief Surveillance Commissioner, Office of Surveillance Commissioners, examined.

Q639 ***Chairman:*** Sir Christopher, good morning, thank you very much indeed for joining us. We are not being televised today but we are being recorded, so could I ask you, please, to identify yourself for the record?
Sir Christopher Rose: I am Christopher Rose, the Chief Surveillance Commissioner. I was appointed to that post almost two years ago by the then Prime Minister and the then First Minister of Scotland.

Q640 ***Chairman:*** Thank you very much indeed. Would you like to make a short opening statement, or would you prefer to continue straight into the discussion?
Sir Christopher Rose: I have no opening statement to make, in the sense that I have any agenda to project to the members of the Committee. I have no agenda. If it would be useful, I could say something about what my office does, but not unless you wish me to.

Q641 ***Chairman:*** That is very kind, Sir Christopher. We have seen, I think, very much, what the office does. Perhaps I could start, if I may, by asking if you think co-ordination between your office and the Interception Commissioner and the Information Commissioner could in any way be improved?
Sir Christopher Rose: Well, I will deal with them separately. So far as the Interception Commissioner is concerned, I think the short answer to that is no, and the reason that I say that is first because as it happens, he and I have known each other as barristers and judges for over 40 years, and neither of us would feel the slightest compunction in picking up the telephone or otherwise communicating with the other. Secondly, we have, more formally, periodic meetings together and with Sir Peter Gibson, the Commissioner responsible for all the security services, when we discuss anything that needs to be discussed. Now I know that this Committee heard some evidence a few months ago from an Assistant Chief Constable which described, if it had happened, a fairly absurd situation when the inspection team from the OSC waved goodbye, as it were, before lunch and the inspection team from the Interception Commissioner arrived at 2.00 in the afternoon. I am bound to say that neither Sir Paul nor I have been able to identify the police force where that is alleged to have happened. It has a slightly apocryphal ring about it, and I have to say that even if it did happen, it was certainly many years ago, and it could not happen now because, for example, my chief inspector, in December of every year, sends to the Interception Commissioner inspector our programme from the following April to March, because we have a much more complicated inspection programme than the Interception Commissioner, for reasons that do not matter. The Interception Commissioner's inspectorate then arrange their visits around us. So if that happened, it certainly could not happen now, and for the reasons which I have sought to explain, I think the co-ordination between Sir Paul and myself is, however surprisingly, not capable of improvement. So far as the Information Commissioner is concerned, I am not at all sure what sort of co-ordination or liaison could exist between us, because the Information Commissioner's role is very different from mine. His, as I understand it, is to promote access to official information and protect personal information. The OSC is operating in a very different field. To put it bluntly, I do not actually have any dealings with the Information Commissioner at all, and I am unaware that he wishes to have dealings with me, though I would be happy to see him if he did.

Q642 ***Chairman:*** Thank you very much indeed, Sir Christopher. The Association of Chief Police Officers has told us that the regulatory framework set out in the Regulation of Investigatory Powers Act of 2000 involves in their view excessive bureaucracy and a burdensome duplication of inspection regimes. Do you think that is valid, and if so, how can it be remedied? Do you think that there is a case for merging some of the inspection activities under one organisation?
Sir Christopher Rose: No to both those questions. First of all, so far as bureaucracy is concerned, I agree with Sir Ronnie Flanagan, Her Majesty's Chief

Inspector of Constabulary, who in a recent report said, "Bureaucracy, like cholesterol, is of good and bad kinds". If you choose to class paperwork as bureaucracy, so be it, but one of the features of the paperwork connected with covert surveillance which is beneficial to everybody is if there is an impeccable paper trail showing what is sought, what is authorised, what renewals and cancellations there have been, that helps everybody. If I may give an example in support of that from my recent experience, earlier this year, at the behest of the Lord Chancellor and Secretary of State for Justice, I carried out a rather swift inquiry into the monitoring of a Member of Parliament when visiting someone in prison, and the general lesson which emerged from that was there was an impeccable paper trail throughout the relevant period showing exactly what had happened and why. So if ACPO or anybody else chooses to say there is far too much paperwork, one has to examine what that actually means. Sometimes, there is excessive paperwork because you will get an inexperienced police officer, for example, who is unduly repetitive either in what he is seeking to have authorised or in what is authorised. That is to be remedied, as it seems to me, by training the relevant officer to do his job better. I think that was a rather long answer to the first question, and for the moment, I have forgotten what the second question was, although I said very firmly no to it.

Q643 ***Chairman:*** Is there a case for merging some of the inspection activities?
Sir Christopher Rose: The answer to that is no, because the job has to be done. The areas which Sir Paul covers are entirely different from mine, and those processes have to be inspected by somebody, so if you had a single Commissioner responsible for everything, there would still have to be the same inspection carried out of the public authority or the law enforcement agency in relation to that particular sphere of activity. I would have thought, particularly in an area which is, partly as a result of the legislation and partly for practical reasons, quite technical and difficult, the more specialism you have among those who are keeping an eye on what goes on, the better the public interest is served.

Q644 ***Lord Peston:*** One of the topics that we are stuck with as a Committee is the public perception of what is called surveillance and the surveillance society. Do you regard it as part of your job to acquaint yourself with what the public views are as to what is going on? Is that part of your remit, or is it not?
Sir Christopher Rose: It would be quite impossible to read the newspapers and watch the television and observe editorial comment without being aware of public perception, but it is not my role, for example, to promote more surveillance or to promote less surveillance. My job, in accordance with the three Acts of Parliament which define what I have to do, is to ensure however much or however little is carried out, it is done properly in a human rights compliant way.

Q645 ***Lord Peston:*** I understood you used the word promote, but you are not even interested as to whether a test of your activity would be whether the outcome involves more or less surveillance; in other words, you are simply looking at the legitimacy of the surveillance?
Sir Christopher Rose: I think I have to be very careful about expressing in public views on subjects which may lead to legislation which at a later stage I will be called upon to express a view about. It is one of the tricks, if I may so describe it, I learnt as a judge, and I keep it.

Q646 ***Baroness Quin:*** Do you feel that you are able, however, to express a view, either a personal or an official view, as to whether there is too much surveillance in our society? We have read the dramatic statements about sleepwalking into a surveillance society; is that something you feel you could say anything to us about?
Sir Christopher Rose: I think it is very important to distinguish between covert surveillance, with which I am concerned, and overt surveillance, with which I am not concerned. I suspect that the man or woman in the street is principally concerned by the large number of CCTV cameras which have mushroomed over the last few years, but unless, in exceptional circumstances, they are being used for a covert purpose, which they might be, they are simply not my responsibility. So far as covert surveillance is concerned, I think it has to happen; it has to happen in relation to serious crime and terrorism, and it does happen, so far as public authorities other than law enforcement agencies are concerned, in relation to matters which many people regard as rightly much less important. Whether a local authority ought to be able to conduct direct surveillance or use CHIS, covert human intelligence sources, for investigating comparatively minor criminal offences is a matter for Parliament not me.

Q647 ***Lord Rodgers of Quarry Bank:*** Sir Christopher, this must be a very naive question on my part, I am maybe alone around the Chair in saying, to ask you a question, what do you actually do? I mean, I know you inspect, but how? Take, for example, I am now not following up the question of local authorities, which follows later maybe, inspections of local authorities, you refer to that; do you actually go into a building and then do you get them to sit down and tell you things, or do you see

papers? If you are inspecting a prison, you see the building and you see the persons, but that is not comparable.

Sir Christopher Rose: I personally do not do any inspections. Can I just give you a nutshell of what my outfit is? There are 27 people in the OSC, of which I am the head. 10 of them are part-time, they are the Commissioners and Assistant Commissioners and me, all of whom are former judges, and we all are part-time engaged. Two of the inspectors work part-time, four of them and the chief inspector work full-time. Then there are ten civil servants who run the office. The actual inspection process is carried out by the inspectors and the Assistant Commissioners. In relation to law enforcement agencies, they are always inspected by inspectors, all of whom, with one exception, are former senior police officers, so if I may say so, they know what they are looking for. If it is a large force, a team of maybe five of my inspectors will go and spend a week with that force; if it is a small force, one inspector will go perhaps for a day.

Q648 ***Lord Rodgers of Quarry Bank:*** Looking at papers or what?

Sir Christopher Rose: Absolutely. It is, if you like, a dip sample of the paperwork in relation to the covert activity which has been carried out during the previous 12 months, and my inspectors, because of their years of experience in the police force, and indeed in most cases their years of experience carrying out this particular job, know what they are looking for in relation to the paperwork. At the moment, I am concentrating on law enforcement agencies. They then report to me, I have a written report, and I either endorse it or I do not. The statutory responsibility is mine, but the nuts and bolts activity is carried out by the inspectors. I then send that report, with or without my endorsement or comments, to the Chief Constable and about two months after that has happened, either I or one of my Commissioners, all of whom were very senior judges, visit the Chief Constable to discuss the report with him. The same sort of principle relates to non-law enforcement agencies, except that we do not, as we do with law enforcement agencies, inspect them every year. Depending on the size of the public authority, and what it is doing, it may be inspected every two years or every three years, but unless something goes wrong, always every three years. The Assistant Commissioners who, as I say, were judges, have historically done the inspection of those public authorities, but now, for reasons I do not need to trouble you with, some of my inspectors will inspect local authorities, just as some of the Assistant Commissioners will inspect law enforcement agencies. Again, it is an examination of paperwork; experience shows that there is a great deal less so far as most public authorities are concerned, because, compared with the law enforcement agencies, they carry out, generally speaking, a great deal less covert surveillance. But again, whoever has inspected reports to me in writing, and then I write to the chief executive, but we do not have a follow-up Commissioner's visit to the chief executive or comparable official of a public authority.

Q649 ***Lord Rowlands:*** You said that some of these issues were for Parliament and not for yourself, but if my figures are right, in 2000, when the 2000 Act was passed, there were only nine organisations allowed to use covert surveillance. Now the figure, which I caught from the press, is 792 organisations. If we have had an explosion of that kind --

Sir Christopher Rose: I do not think, with great respect, that your figures are right.

Q650 ***Lord Rowlands:*** It is the Daily Telegraph's figures actually.

Sir Christopher Rose: There are over 60 law enforcement agencies which have been carrying out covert surveillance since the Police Act in 1997. The Regulation of Investigatory Powers Act and its Scottish equivalent spread the power to, as you rightly say, many hundreds of public authorities, but that was in the original legislation in 2000. Now it is only over the years since then that some, not all of them, have used those powers, but they have been empowered to carry out covert surveillance -- I am open to correction, but I am pretty confident -- since the original legislation in 2000.

Q651 ***Lord Rowlands:*** The reason I am raising it, it would be a matter for concern, because the variability in the quality, when you increase that number of organisations capable of exercising these powers, is going to cause and probably will cause concern, does it?

Sir Christopher Rose: Well, it would cause concern if there was widespread incompetence in carrying out covert surveillance, but that is what my outfit does its best to prevent. That is why we inspect all these bodies, and try and get them to a uniform standard of compliance. I have to say that we have proved a great deal more successful in relation to law enforcement agencies than we have in relation to some public authorities.

Q652 ***Lord Rowlands:*** Just one final point, it is the same Daily Telegraph piece, and I hope you will either correct it or -- there is a story here of Poole Council or Authority using the powers in the 2000 Act to spy on parents because they thought they were not in the school catchment area, and also to spy on, as this account says, on shell fishermen, shellfish people. Would you be able to check whether they are

obeying the law correctly and behaving properly in that respect?
Sir Christopher Rose: Yes, whether they would be carrying out that spying, as you put it, lawfully would depend on what the shell fishermen, for example, were suspected of doing. If it was a criminal offence, then the local authority would have the power to do that. So far as my check on what goes on is concerned, as I said earlier, all we can do, we are a tiny outfit, is a dip sample, when we inspect that or any other particular authority, and if they have done it -- of course, if they have chosen to do it improperly, without any paperwork, there will be nothing for us to inspect, but I have no reason to believe that any public authority would be foolish enough to embark on that sort of conduct, particularly as the consequences under the Human Rights Act would be pretty serious. So if the paperwork is there, then yes, my inspectors will look at it.

Q653 ***Lord Rowlands:*** So if a press report like this occurred, you would also respond possibly to it, by saying, "We had better go and check this out"?
Sir Christopher Rose: Certainly not. It would be totally impossible to do that. As I say, there are a very large number of authorities which we inspect, we have a carefully designed programme. I mean, I am not ruling it out absolutely, if there was a well documented manifest abuse of power by a local authority, well then, of course we would try and do something about it, but I am afraid responding to press reports is not always a fruitful activity when you only have a small amount of resources at your disposal.

Q654 ***Lord Morris of Aberavon:*** I appreciate that, Sir Christopher, that you only have a small office, and obviously the field is large. You say in your report, paragraph 5.5: "At inspections all aspects of covert activity are examined and the findings reflect the evidence from a small random sample of documentation . . . " This I understand, but is it adequate? How do you know it is adequate, the kind of dip sample you referred to a few minutes ago?
Sir Christopher Rose: Well, I cannot prove that it is adequate, because the 10 per cent of documentation, or whatever it is in the particular case, which is examined may or may not be representative, so I cannot prove that it is adequate.

Q655 ***Lord Norton of Louth:*** You mentioned obviously there are a large number of bodies that engage in surveillance; another point of course is there are different types of surveillance that can be undertaken, and they require different types of authorisation. So the question is: does that cause any operational confusion, and is there a case for actually having greater consistency when it comes to authorisation?
Sir Christopher Rose: I think the answer to that is no. I think that the lesson from the law enforcement agencies, which as I earlier suggested is not as well learnt by many public authorities, is that there is no confusion. Those who are involved in the authorisation of covert surveillance know what kind of authorisation is required for what kind of surveillance as prescribed in the legislation and the Codes of Practice. So far as the law enforcement agencies are concerned, all of them, I think I can say now, with no obvious exception, take seriously their responsibilities to act essentially in a human rights compliant way, which is what this is all about, and they have gone to considerable lengths to provide the training so that their officers who are doing this job know exactly what they are doing. That, I may say, is not a product of the seniority in rank of the officer; you may have a constable who is far more experienced and skilled than some chief constables in relation to what is required with regard to particular authorisation. Other public authorities I am less confident about. As I have said, very few of them carry out covert surveillance on a large scale, but I have to try and ensure that even if they do not do it at all, they know how to do it, so that is the purpose of my inspection.

Q656 ***Lord Norton of Louth:*** The problem is not the level of authorisation, it is the point you make in your report, it is, if you like, the lack of knowledge about what is expected of them.
Sir Christopher Rose: Yes, and that comes basically down to training.

Q657 ***Lord Peston:*** Just briefly, I found your answer to Lord Rodgers highly enlightening as to what you actually do, but could I give you an example? Supposing you are going to a major police authority, with these very senior people from your side going there, I think you said there might be five of them, supposing the following hypothetical thing arose, that one of them spoke to whoever he was dealing with and said, "Are you engaged in any covert surveillance of a major criminal?", just a straight question, is that perfectly proper behaviour on their part?
Sir Christopher Rose: To ask the question, yes.

Q658 ***Lord Peston:*** To just go straight, "Are you doing that?"; what about then if the senior policeman he is talking to says, "Yes, we are doing such a thing, that is one of the things we are currently doing, but this is so delicate, and it could so easily go wrong, that we really do not want to tell you about it". Would that be an acceptable answer to you?

Sir Christopher Rose: It may be.

Q659 ***Lord Peston:*** Because their worry would be even with your level of excellent people, something can still leak out if it gets beyond the narrowest of circles; you would accept that as an answer possibly?
Sir Christopher Rose: It may be acceptable, it would very much depend upon the level of officer who was giving that answer, and if my inspector had concerns -- because there may be, one has to be alive to the fact, rogue police officers who may or may not be carrying out covert surveillance in the wrong way. If my inspector had a cause for concern for any reason, he would report it to me, and I would raise it personally with the Chief Constable. Now the scenario which you mention is the sort of thing which could be addressed in that way.

Q660 ***Lord Lyell of Markyate:*** Sir Christopher, I am going to ask you if you can please explain what is involved in directed surveillance, but before I do it, can I just put a little flesh on the thing? Your report is extremely interesting, and if I may say so, your small office seems to be doing a very good job of training, coercing, encouraging particularly public authorities, but a whole raft of authorities with which you deal, to go down the right road. If I use the word opaque, I do not mean it rudely at all, you inevitably write in very careful legal language. It is not very easy to link that with people's day-to-day concerns, and you rightly read the newspapers, and I got the library to produce the sort of last six weeks of comment. What people are worried about is whether covert surveillance is now being used on them for pooper scooping of dogs, cheating on the disabled badge, the shell fishing case in Poole, the question whether people are abusing school catchment areas, fly tipping -- personally I would snoop as much as I could, because I think they are an absolute menace -- and people chucking cans from cars. Now it looks as though a good deal of partially covert, partially overt surveillance is going on in those areas. Is this what you have to concern yourself with, and how does that tie in with the question of directed surveillance, because people are worried that there is more and more of it?
Sir Christopher Rose: Well, directed surveillance is defined in section 26(2) of RIPA. It has essentially five elements. First, it is covert, that is to say it is calculated to ensure that the target is unaware of it. Secondly, it is not intrusive; intrusive is defined in the legislation as being the entry of residential premises or a private vehicle which involves the presence of a person or a device in the residential premises or the private vehicle. Thirdly, it is undertaken for purposes of specific investigation, that is to say it is focused on a particular individual or individuals. Fourthly, it is conducted in a manner likely to obtain private information. And fifthly, that it is preplanned rather than an emergency or urgent response to some sort of activity. The sort of areas that you have specifically mentioned can only lawfully be the subject of direct surveillance by a public authority, leaving aside law enforcement agencies, if it is carried out for the purpose of preventing or detecting crime, or of preventing disorder, because that is the only one of the seven grounds of necessity for directed surveillance set out in section 28 of the Act which is open to a public authority.

Q661 ***Lord Lyell of Markyate:*** Could I just follow up on the specific example of the family, and many of us will have read about this, in I think Poole again, where the local authority was trying to show that they were cheating on whether they lived in or outside a catchment area, and they had been contemplating moving house. It is quite well set out in the Daily Telegraph in April, and I can supply your office with it, but it seems worth following up, because except that they say there may be fraud, because they might have told a lie possibly, I very much doubt if they did, from reading the press, but it looks as though covert surveillance was being used on this question of catchment areas, and I think that sent a bit of a shiver down my spine, although I have no children going to school at the moment, and I think that is the kind of thing that worries people; is your office on top of it?
Sir Christopher Rose: I have three points to make in answer to that. First of all, that sort of activity could only be permissible under RIPA if it was going to lead to the prevention or detection of crime, which no doubt leads to the suggestion of fraud. The second point to be made -- I do not, I am afraid, carry in my head when Poole District Council is due next to be inspected, but you can be quite sure that when they are, they will be aware of the point which you make, of which indeed, I have to say, whether they are readers of the Daily Telegraph or otherwise, they already are aware. But what I cannot do, and I touched on this at an earlier stage, I cannot say, "We will inspect Poole next week".

Q662 ***Baroness O'Cathain:*** Sir Christopher, reading through your report, there was an item on page 12, paragraph 8.9, where you said you had been disturbed by the introduction by some forces of the term "tasked witness" as an apparent alternative to the correct legally recognised term "covert human intelligence source". First of all, what are the origins of that term, because it does seem rather strange, but is it the police force who actually decide to do that themselves, and to engage these people? Do they not have some sort of responsibility to liaise back with you, that they are doing so, because it seems to be outwith the normal procedure of dealing with covert surveillance in police forces.

Sir Christopher Rose: Point one, in answer to your question, whatever the nomenclature, whether tasked witness or CHIS or anything else anybody comes up with, any person who is being used in a way which is within the statutory definition of a CHIS must be treated as a CHIS and afforded the same risk assessments and so on. Point two, the phrase "tasked witness" comes from the police, it has been used by them to identify someone who, unlike an ordinary informant who is a CHIS, will give evidence in court. CHIS, almost by definition, will not. So far as the legislation and my role is concerned, I do not care whether they are going to give evidence in court or not, but if they are being used and potentially abused in a way within the statutory definition, then they have to be treated as a CHIS, and there has to be the appropriate handling mechanism and supervision mechanism. Last point three, in answer to your question, there have been some very fruitful discussions in recent months with ACPO on this very subject, and the short answer is that they now understand that whatever they call these people, they have to be treated in accordance with the legislation.

Q663 ***Viscount Bledisloe:*** I just wanted to go back to the question you were asked earlier about the person who was too sensitive to investigate for the moment. Would you go back and investigate about that when the sensitivity had passed?
Sir Christopher Rose: I am afraid the only answer I can give you to that is it all depends. It would depend on all sorts of circumstances. But as you will understand, partly in answer to your question, and partly in supplementary answer to what I said before, it is of the essence of a highly sensitive inquiry that the fewer people who know about it, the better, and that must, as a general principle, extend to my inspectors as well, because although one hopes that one's inspectors are incorruptible and are uncorrupted, there are such sensitivities involved in some forms of covert inquiry that it would be entirely wrong for the police force to disclose a particular matter.

Q664 ***Lord Morris of Aberavon:*** Sir Christopher, may I ask you, how are the tests of proportionality and necessity applied to the kinds of surveillance that fall within your supervision?
Sir Christopher Rose: Well, so far as necessity is concerned, one has to be a bit careful, because the definition in section 93 of the Police Act is different from the considerations which arise under RIPA. Under the Police Act, the test for property interference or intrusive surveillance in relation to necessity is whether the surveillance is likely to be of substantial value in preventing or detecting serious crime, that is violence, substantial financial gain, many people with a common purpose, or activity likely to attract a sentence of three years or more for someone who is 21 years old, and that objective cannot be obtained or achieved by other means. Now that is necessity when one is considering it in relation to that Act. Necessity under RIPA is the seven categories which are set out in section 28(3), one of which we have already talked about, which is what public authorities can do, in relation to preventing or detecting crime or preventing disorder, but the first ground of necessity, unsurprisingly, in that sub-section, is the interests of national security; and the third ground is in the interests of economic well-being. I will not bore the Committee by reading all seven of them, but there are seven grounds to underpin necessity. So far as proportionality is concerned, the methods used have to be proportionate to what is sought to be achieved, and so authorising officers, whether of law enforcement agencies or other public authorities, when they are deciding whether to authorise particular activity, have to balance the intrusiveness of the activity against the operational need, and that is something which can be found in the Code of Practice. For example, using a sophisticated aerial spying device or staking out premises from six different vantage points may be proportionate in relation to murder or indeed terrorism, but wholly disproportionate if one were concerned with petty receiving or benefit fraud. So the responsibility in relation to the balancing exercise and the assessment of what is necessary and proportionate in order that the activity be Human Rights Act compliant rests upon the authorising officer, and he or she has to carry out that balancing exercise before authorising or not, as the case may be, and that relates essentially across the board to whatever kind of covert activity is involved.

Q665 ***Lord Morris of Aberavon:*** Am I right in thinking that as part of your inquiry into the samples, you would be looking at the balancing exercise and how it is done?
Sir Christopher Rose: Yes. I say that with complete confidence, because that is exactly one of the things which my inspectors look at.

Q666 ***Baroness Quin:*** You partly touched on my question in your earlier reply to Lord Norton, where you talked about the importance of training. But could I just press you a little bit about what part does learning about human rights and privacy protection play in the training? Are you satisfied that this part of the training is adequately addressed?
Sir Christopher Rose: I can tell you what part it should play. What part it does play varies according to the quality of the training which is given. It is fundamental that those who are carrying out covert activity recognise that that is a breach of privacy and a breach of the right to family life under Article 8. That is stage one of the training, that is fundamental.

Stage two is that they must recognise that if what they do is not necessary and proportionate, then there will be a breach of the Article 8 rights. And thirdly, and this really is the bottom line, because it should be the object of all covert activity, the litmus test is: will a trial judge admit the product in court? It is not very likely that he will if it was obtained in a disproportionate or unnecessary manner, or was otherwise unfair. So my answer to your question is that is the bedrock of the training which should be provided, and that message, I am reasonably confident, is well understood in all law enforcement agencies, it is well understood in some other public authorities, and I regret to say not as yet, despite the fact that the legislation has been there for eight years, understood at all well by a minority of public authorities.

Q667 ***Baroness Quin:*** What can be done in the case of the minority of authorities, in order to ensure that they do address these issues?
Sir Christopher Rose: Well, I do not have any power of sanction save to report to the Prime Minister. That has happened historically on very few occasions in relation to law enforcement agencies. I do not believe that my predecessor reported a public authority, I have to tell you that I am on the verge of reporting a public authority, and the reason for the difference is partly the degree of activity which takes place, because the law enforcement agencies are the people who do most of it, and comparatively few other public authorities do much of it, and they are only inspected much less frequently. But when the stage is reached, as I have to say it seems it might be reached quite soon in relation to a particular public authority, where despite what their chief executive has said they will do, they have not done it, then I shall report it to the Prime Minister. What the Prime Minister does about it, of course, I could not possibly speculate upon.

Q668 ***Lord Rowlands:*** Your report does in fact throw some light on the question of the available quality in the local authority area, to return to this, but can I just clarify the point, your inspectors, do they check the training programmes that are in place, when you go in for an inspection?
Sir Christopher Rose: They do not, as it were, sit in on a training session, no, but they can see from the documentation which is deficient whether training is necessary, and their report --

Q669 ***Lord Rowlands:*** They report that to you?
Sir Christopher Rose: They report it to me, and I say, "Come on, chief executive, address this", and if the next time they are inspected they have not, then that can lead to the path I have just been exploring with Lady Quin.

Q670 ***Lord Rowlands:*** So there is a proper process by which, through inspection, you could drive the quality and standards of training up?
Sir Christopher Rose: Absolutely, and that is what has actually happened, conspicuously, as I say, with law enforcement agencies, less conspicuously with public authorities, in the eight years since the legislation came in.

Q671 ***Lord Lyell of Markyate:*** That brings me back to the second part of my main question that I did not expressly put to you: does the large increase in the numbers of directed surveillance authorisations granted to non-law enforcement authorities, in other words public authorities mainly, pose a potential threat to the rights of the citizen?
Sir Christopher Rose: Well, your premise is an interesting one, because yesterday, I looked at the statistics which in due course will be in my annual report for this year, which I hope will be published in July, in relation to directed surveillance, and although so far as law enforcement agencies are concerned, the amount of activity during the last 12 months has been very closely comparable to the previous 12 months, there has been a very conspicuous drop so far as other public authorities are concerned. Insofar as I can remember them, I will give you the figures, because when I saw the question, my impression from reading the newspapers and so on was that there had been a great increase; not so. During the last 12 months, up to the end of March, there were roughly 9,500 authorisations for directed surveillance by non-law enforcement bodies. The previous year, there were 12,500. Equally, at the end of last year, there were 1,200 authorisations still in force; at the end of the previous year, there were 1,800 authorisations then in force. So the statistics that I have, which I hope are reliable, of course some local authorities do not bother to reply, however often they are chased, but I think we have had about a 90 per cent response with the statistics, so I hope those are reliable. So rather surprisingly, they suggest there has been a decrease rather than an increase. As to whether there should be more or less surveillance by public authorities other than law enforcement agencies, I really have to retreat behind the answer which I gave at an earlier stage, that is a matter for Government and Parliament, not for me. My concern is to ensure, however much or however little, it is done properly.

Q672 ***Lord Lyell of Markyate:*** Perhaps I could comment that hopefully they are taking rather more notice of what seems to be public concern in the area.

Sir Christopher Rose: That may be.

Q673 ***Viscount Bledisloe:*** In paragraph 11.3 of your report, you say that the speed of change in improving technology often surpasses the limitations of current legislation, and you cite automatic number plate recognition as an example of that. Presumably improvements in technology continue and are likely to continue. What solution do you see to this problem? Are they going to have to legislate every time in relation to each particular advance, or can we think of a more comprehensive solution?
Sir Christopher Rose: I think the problem arises from the statutory definition of what is intrusive. What is intrusive for this purpose is if you have a device which is capable of providing you with information of the quality which you would get if you were yourself in the motor car or in the house. ANPR highlights this particular problem, because in 2000, when the legislation was passed, the technique was adequate for recognising number plates. The technique is now capable of identifying not only the number plate, not only the driver, not only the front seat passenger, but the back seat passengers as well. This raises a variety of problems, one of which is anybody driving their car on a motorway where they know there are cameras will expect nowadays that the number plate of the car will be capable of being recognised, so that is not covert, nor is it intrusive. But what many people would not expect is that there is the capacity to see exactly what is going on in the motor car, and that comes within intrusive surveillance, so the original old-fashioned device of number plate recognition is not intrusive, there is the capacity now for intrusion. There is a divergence of view, I have to tell you, between the Home Office and me, you will not be surprised to learn, as to whether legislation is necessary. The view taken by my predecessor, and by me, and by all my Commissioners, all of whom, as I say, but one are former Court of Appeal judges, so we may have something helpful to say about the law, is that the present legislation is too blunt a tool by its definition of intrusive surveillance to deal with that particular problem. There are others which arise because of improved technology.

Q674 ***Viscount Bledisloe:*** So you recommend that a new definition of intrusive would provide a general solution to this problem rather than having to have special legislation each time there is a new invention?
Sir Christopher Rose: I hope that it would, but I hope you will not mind my saying that my experience of legislation in 21 years as a judge was that it did not always achieve that which it was intended to achieve.

Q675 ***Viscount Bledisloe:*** A masterpiece of understatement, Sir Christopher. This, I think, is tempting you somewhat past the barriers you put up, but you point out that your writ does not extend into private prisons, prisons that are privately managed.
Sir Christopher Rose: Yes. That, I think, is the subject of legislation at the moment. Forgive me, I cannot give you chapter and verse off the top of my head, but there is something moving on that. I do not know whether it is by way of statutory instrument or otherwise. Unless I have misremembered, I think something is happening on that front.

Q676 ***Viscount Bledisloe:*** What, to bring private prisons within your scope?
Sir Christopher Rose: Yes, exactly, because public prisons are of course -- it is the privately-run ones that cause concern.

Q677 ***Chairman:*** Sir Christopher, you have been extremely generous with your time, thank you very much for attending and giving your evidence.
Sir Christopher Rose: I have to confess that it is the first time in my life that I have answered rather than asked questions in public. You have been very kind.

Examination of Witness

Witness: Sir Paul Kennedy, Interception of Communications Commissioner, examined.

Q678 ***Chairman:*** Sir Paul, may I welcome you very warmly to the Committee? I see you have already been attending our proceedings. We are not being televised but we are being recorded, so could I ask you please very kindly to identify yourself for the record?
Sir Paul Kennedy: I am Paul Kennedy, the current Interception of Communications Commissioner. I was appointed by the then Prime Minister in April 2006 for a three-year period, and I succeeded Sir Swinton Thomas in that office. Previously, I was a member of the Court of Appeal.

Q679 ***Chairman:*** Thank you very much, Sir Paul. May I start by asking a similar question to that which I asked the Surveillance Commissioner, if you think that the co-ordination between your office and those of the Chief Surveillance Commissioner and the Information Commissioner could be improved.
Sir Paul Kennedy: One of the reasons for my being present previously was to hear what he said. As he said, we have known each other a long time, and the short answer is so far as he is concerned, I cannot see any way in which it could be improved. We know each other perfectly well, our offices work together,

and like him, I have had practically no contact with the Information Commissioner, so I do not see any point of stress in that area. In substance, I adopt what he said to you, in answer to the same question which you posed to him.

Q680 ***Lord Smith of Clifton:*** What happens if the two Commissioners were not from the same stable, did not know each other, and were not engagé to the extent you are?
Sir Paul Kennedy: I think the answer is really in what Sir Christopher said a little earlier on, and that is we are dealing with different functions. I wonder if I may elaborate slightly on that. I am concerned with Interception of Communications, and that means an audit function, as in his case, but an audit function in relation to a wholly different type of operation. In the course of, for example, a police inquiry, it may be useful to use different tools, and therefore, I can see that from their perception, there are two different types of inspection. But on the other hand, interception is wholly different from surveillance, and because it is wholly different, one uses different methods to inspect what has happened, and there is no difficulty about us keeping our functions entirely separate, because we are looking at different operations. I do not know whether that helps.

Q681 ***Chairman:*** Can I also ask Sir Paul the question that I put earlier: the Association of Chief Police Officers has told us that the regulatory framework set out in the Regulation of Investigatory Powers Act 2000 involves excessive bureaucracy, and a burdensome duplication of inspection regimes. Do you agree with that, and if so, do you think there is any way in which it can be remedied, and if there is a case for merging some of the inspection activities under one organisation?
Sir Paul Kennedy: I do not agree with it. Like Sir Christopher, I think that it is particularly important when, rightly, the public are sensitive to the sort of activity which is going on, that if there is anything to be investigated, there is a clear audit trail, and if you are going to have a clear audit trail, you have to have some sort of record of what happened. Now my inspectors have been very anxious to ensure that so far as possible, the record does not go further than it needs to. One of the things that happened as a result of consultation was that the form used for recording an application to make some kind of record of data was simplified, and surprisingly, in the light of what you were told, one of our big difficulties has been persuading certain authorities to use the simpler form, because the older form tended to be duplicating certain pieces of information, and it was wholly unnecessary to do so. The other thing we have been encouraging people to do, and indeed my predecessor did as well, is to use electronic communication where possible. So far as I am concerned, I have no interest in them keeping bits of paper, except for the original warrant, provided there is a proper audit trail which can be recovered if need be when an inquiry takes place, and the value of that, as Sir Christopher said, was demonstrated by the inquiry which he carried out when it was possible to say this activity had plainly been authorised by this person at this time and covered what happened.

Q682 ***Lord Smith of Clifton:*** Sir Paul, would a requirement for judicial rather than ministerial authorisation of intercepts improve the safeguards for the citizen, and what would be the downside of such an operation?
Sir Paul Kennedy: I recognise, first of all, that other countries have different systems, so nothing I say is intended to be derogatory of anybody else. On the other hand, I am entirely happy with the way in which our system operates, because I think it actually provides to some extent more safeguards. If you have a judge to whom an application for a warrant is originally sent, that judge, or if it were more than one, two judges are going to be necessarily security cleared and are going to be the judges used for that purpose. They become, in a sense, a part of the system. I think there is a positive advantage in not being a part of the system, being a part-timer who comes to audit what has happened. Furthermore, as things happen at present, the application for a warrant to intercept goes to the Secretary of State, the Secretary of State is answerable to Parliament, and therefore, there is someone who is accountable in a way that a judge in that position would not be accountable; and, for what it is worth, part of my function is to audit what has been done by the Secretary of State. So overall, I believe that we have a system with which we should be content, and there is no particular reason to change to the sort of system used elsewhere.

Q683 ***Lord Smith of Clifton:*** But it is sometimes mooted, Sir Paul, that there is a greater confidence among the public at large if judicial permission is given rather than ministerial, because there is a more independent assessment of the application, and that is why it is sometimes mooted from time to time, even by the Government itself, that it would be better to have a judge hearing these authorisations than a minister.
Sir Paul Kennedy: I see the argument, I just believe that these are two possible standpoints, and there is a great deal to be said for where we are, because I think, as I said to you, you do have the judicial input, but it comes in separately, and there is a great deal of independent scrutiny in relation to the operation as it

exists now. Would it help if I amplified a little bit on the way in which the work --

Q684 ***Chairman:*** Thank you.
Sir Paul Kennedy: There are two sides to the operations with which I am concerned, which it is very important to keep separate, and which I am afraid, after the publication of my last report, were not entirely kept separate by certain parts of the media. One is interception, that is what somebody said to somebody else, very often on the telephone, or going back a little historically, in a letter. The other is data, which is who telephoned who. So far as interception is concerned, it is necessary to obtain a warrant from the Secretary of State. In order to obtain a warrant, an application has to be made, and the application will be carefully scrutinised at several levels. If it has come, for example, from a police force, it goes through the various processes of scrutiny internal to the police force, I am speaking in very general terms, and then internal to, for instance, the Secretary of State for the Home Department. If she signs the warrant, then of course I may inspect that warrant and the information given to her in order to support that, and that is very much part of my function. If it is, by contrast, data, then a police force may wish to obtain a telephone number, they know what the telephone number is, they merely want to know who is the person who owns that telephone number, that can be obtained without it going anything like so high up the ladder. It has to be obtained by means of a superintendent giving the necessary authority, but the superintendent, by definition, will not be somebody who is engaged in the particular inquiry which is then afoot. That gives the degree of independence at that level. So there are two wholly different functions, but it seems to me that the way in which each goes up the ladder provides its own checks against somebody going off on a frolic of their own.

Q685 ***Lord Rowlands:*** It leads me to ask the question, in paragraph 58 of your report, there are these "requests for communications data which totalled 253,557"; it sounds to the average layperson an enormous number.
Sir Paul Kennedy: Sorry, can you direct me to the paragraph?

Q686 ***Lord Rowlands:*** Paragraph 58, page 11. To someone reading that cold on the issue, it sounds an enormous number.
Sir Paul Kennedy: It builds on what I have just said, of course. Those are requests for communications data, and they can be very frequent and numerous, but they on the whole, as far as we can see, are justified. That is part of our function in carrying out the audit.

Q687 ***Lord Rowlands:*** Has that figure been going up? Has there been a significant increase from one year to the next?
Sir Paul Kennedy: From memory, not enormously, though there has been some increase. I did not do the same enquiry that Sir Christopher did, I cannot remember what the figure is for the year ended last December without checking, so I cannot tell you whether the figure in the next report, when it comes out, will be slightly higher than that.

Q688 ***Lord Rowlands:*** Just to clarify, the figure is the number of requests to say, "Yes, please can we know this telephone number?", is that right?
Sir Paul Kennedy: Yes, I am putting it very broadly, but yes, it is for communications data, not for intercept, that is the important point. The requests for intercept figure is much lower.

Q689 ***Lord Rowlands:*** So it could be a number of requests for the same telephone? Are there going to be 253,557 individuals affected, as it were?
Sir Paul Kennedy: No, it is not in relation to an individual, it is a composite figure for all of the police forces, local authorities et cetera who have sought information which is recorded by communications service providers, that is really what it is.

Q690 ***Lord Rowlands:*** You are saying we should not be phased by that apparent size of number?
Sir Paul Kennedy: I do not see any reason -- this sort of information is immensely valuable. The local authorities were criticised to some extent for using the powers which we regulate, but one county council, I am looking at a document produced by the local authorities themselves, used telephone records to track down and successfully prosecute a car clocking gang which had made £4 million selling clocked cars to unsuspecting buyers. That seems to me to be precisely what they ought to be doing. So I have no anxiety about the use of the powers.

Q691 ***Baroness O'Cathain:*** Can I just ask, are these numbers not available, like everybody else gets them, on the internet?
Sir Paul Kennedy: Some of them are, not all.

Q692 ***Baroness O'Cathain:*** So you are just redoing Directory Enquiries, are you?
Sir Paul Kennedy: By and large, if they are available that way, their own managers do take care to ensure that that which can be obtained easily another way is not duplicated.

Q693 ***Baroness O'Cathain:*** So it is not really significant?

Sir Paul Kennedy: The degree of ingenuity of those who operate in this particular twilight world should not be underestimated.

Q694 ***Lord Peston:*** Some of us were brought up with John Stuart Mill's great dictum in mind -- he does not use the word decent society, but he uses some expression: there is a private space for each individual into which no government of any kind can intrude. Am I right that the mere existence of your office says that John Stuart Mill simply does not apply in our society? That is my first question.
Sir Paul Kennedy: Right across the board, yes. I think we can no longer --

Q695 ***Lord Peston:*** So what we have here is a really clear-cut case of a great philosopher whose contribution has come to an end.
Sir Paul Kennedy: I think if you are saying that in an age where people can suffer what London suffered on the day when a lot of bombs went off, I am just afraid -- it is a decision of Parliament, but it seems to me to be an understandable decision of Parliament, that you have to accept that we have to do what we can to prevent it, and that may mean and does mean that nobody -- I entirely accept that properly authorised by the Secretary of State, my telephone conversations can be intercepted, why not?

Q696 ***Lord Peston:*** Some of us take an opposite view, you may not be surprised to know, because Mill did not say "in certain circumstances", he said in any society whatsoever, no matter what the circumstances. We were told last week, I did not understand the technology, something about parabolic microphones, where they can eavesdrop all over the place listening to conversations, that is not just in public spaces, they can direct them at private spaces. I am not quite clear -- I have never seen one, but I assume they are a very sophisticated listening device. Does that fall within your remit?
Sir Paul Kennedy: Yes, in one sense, in that if you are seeking to intercept a conversation, yes, because that is what Parliament has laid down, that my office is responsible for interception of communications.

Q697 ***Lord Peston:*** Is the purchase and sale of such technology -- presumably you can get involved with that as well. I do not know how you buy a parabolic mirror, where you go or anything.
Sir Paul Kennedy: Nor do I, therefore I am not pretending to offer any confident answer to that, but if devices of that kind are used to intercept communications, yes, they would fall within my remit. I can put it the other way round: section 1 of the Act forbids it, and it is a criminal offence to intercept.

Q698 ***Lord Peston:*** Well, exactly.
Sir Paul Kennedy: So it only becomes legal if you have a warrant to do it, and if someone sells such a device and somebody else uses it, they are committing a criminal offence.

Q699 ***Lord Peston:*** And you would then be involved?
Sir Paul Kennedy: No, because that is a criminal offence.

Q700 ***Lord Peston:*** I understand, forgive me.
Sir Paul Kennedy: The police ought to be involved, but not me.

Q701 ***Lord Morris of Aberavon:*** Sir Paul, on the question of ministerial authorisation, and we have a constant pressure in the House for judicial supervision, which I am in a great deal of sympathy with, but you make your report to Parliament, via the Prime Minister, but I note in paragraph 9 that, other than a Scottish minister, you have not in your period of office met any other minister, and they are set out here in some detail. Is that deliberate, or is it important that you are seen to be apart?
Sir Paul Kennedy: No, it has wholly changed since the report was written. That was written after I had been in office nine months, and due to diary commitments, it had not been possible to see a number of people. I have now seen, I think, every single one of them; if not every single one, all but one. The object of seeing them personally is to make sure that they are satisfied with what is presented to them for the purpose of obtaining the warrant, and I, for example, ask if they have ever refused one. I would not expect them to refuse them very often, because of the filter process I spoke about earlier. I would hope that people would know what the Secretary of State ought to be persuaded to support, but I can think certainly of one where the answer was yes, and there I took deliberately the step of ensuring that I got that file when we next did the inspection, because I wanted to see how the line had been drawn.

Q702 ***Lord Lyell of Markyate:*** Just quickly back to these parabolic microphones, I am no expert, but I certainly understand they exist, and they can be quite effective. Would they be more likely to fall within the realms of Sir Peter Gibson and the security services? I am slightly surprised it has not crossed your desk as a potential abuse.
Sir Paul Kennedy: Well, in a sense, the answer to that is probably what I have just given, that it is not a misuse of intercepting power, it is not something that is part of my remit. I am concerned with whether or not the lawful use or what is purportedly lawful use has been made according to the rules which have been laid down. Once you start from the proposition that

any interception is illegal, it is not part of the Commissioner's remit at all. It only comes within my sphere of activity once the warrant has been issued. So you may be right, maybe Sir Peter Gibson has had some dealings with it. I have not. I am conscious, like you, of the existence of it, but only in the very vaguest terms.

Q703 ***Lord Lyell of Markyate:*** It comes down to this, does it, that so long as people are trying to obey the rules, you are there keeping an eye on it, but if they deliberately ignore the rules, then your office is no protection to anybody.
Sir Paul Kennedy: Well, the police are, we are back-to-back. If you do not obey the rules, you are committing a criminal offence.

Q704 ***Lord Lyell of Markyate:*** And who investigates it?
Sir Paul Kennedy: They do.

Q705 ***Lord Lyell of Markyate:*** The police, if they know about it?
Sir Paul Kennedy: If somebody intercepts, without a warrant, no doubt it is technically possible, then the police would intervene. Having said it is technically possible, perhaps I should just say a little bit more. I do not want to go too far down this route for obvious reasons, but the mechanism is that the warrant having been obtained by whoever it is, MI5 or the police, the information has to be provided, and the only person who can provide it are the communication service providers. So in this sense, one is totally different from Sir Christopher's remit. They will only provide it if there is a warrant in existence. So the risk of it being obtained by some rogue element in that way is relatively small. What I thought was possible, I know too little about what is, as it were, at the frontiers of where we are going now, is whether there would be some way of cutting them out of the system. As far as I know, there is not. But we operate therefore within really what is a ringfenced system, and one of the ways in which my inspectors dealing with data operate is that before they go to a police force, they get in contact with the major communication service providers and they say, "Tell us about the applications for data which you have received from whichever police force it is", and they then select at random from what they get back from the communication service providers a number of those particular applications.

Q706 ***Lord Rowlands:*** Could you clarify what these communication service providers are?
Sir Paul Kennedy: O2, BT, all the big names you know about, and the Post Office. But armed with what they have got from Vodafone, O2, they then go to the police force and they say, "We would like to see that file and that file and that file", which seems to us to be quite a useful check, because it means that on any view, the police know that they are at risk in any given case of the inspectors getting the lead-in not from them but from the person to whom they have had to apply in order to get the information back. In a rather similar way, though not quite the same, before I -- and I should perhaps again draw the difference, I do the inspections personally in relation to about nine, and that is I think where the figure came from, bodies who are entitled to seek interception information. So I go to MI5, the Customs and Excise, the SOCA, the Serious Organised Crime Agency and so forth, and before I go on these type of inspections, I get a list of all the warrants from them which they have, and I pick from those at random, because there are a sufficient number that it would not be possible in practice to inspect them all. But again, that means one is hopefully getting a cross-section of what goes on, and equally from the point of view of each of those who are inspected, they know that I might pick any one, so they hopefully will be doing the same in relation to the ones I have not seen that they have done in relation to the ones I have.

Q707 ***Viscount Bledisloe:*** You, like Sir Christopher, have to look at the questions of proportionality and necessity. Do you do so in the same way as he does, or is there any variation between your two offices because of your different roles?
Sir Paul Kennedy: I think the answer is substantially the same. I can put it rather more simply, in a way: necessity relates to the operation itself. There must be a need for the operation in relation to national security, crime or economic well-being of the country. It may be that this inquiry is necessary legitimately in relation to one of those targets. Then the question is, is it proportionate? Are we using, in very colloquial terms, a sledgehammer to crack a nut, and it is not justifiable? I think that is the way in which one would expect everyone to operate. It is underlined by the Human Rights Act.

Q708 ***Viscount Bledisloe:*** Do you think that the people asking for the right to intercept really have mastered the concept of proportionality, and that they understand the safeguards and the Codes of Practice?
Sir Paul Kennedy: It has improved enormously. One of the things that has happened is that under the umbrella of West Mercia Police Force, there is a training organisation which, first of all, came into existence, but then has been training key figures, particularly initially in relation to the police, which is the single point of contact. You can see I have been, because they gave me a bag. But that has enabled the key officers to have a much better idea of what in fact

they ought to be doing. They have now moved on to dealing with those at a slightly higher level, who are essentially the ones who are giving the permission. The way in which the inquiry works, as you may well know, in relation to the police, is that if the officer on the ground, who is the investigating officer, thinks this might be a useful line of inquiry, he or she makes her approach to the senior single point of contact, who then provides, as it were, the necessary expertise, "This is the way we ought to be going", and helps to shape it. Indeed, in relation to a complicated criminal inquiry, one would hope that a single point of contact officer would be assigned to that inquiry at a fairly early stage to provide that kind of input. But having shaped the application, it will then be presented to the designated person, at the rank of superintendent, who then has to decide whether or not it is going to be authorised. West Mercia are now doing courses for designated persons as well as for single points of contact, so you are getting this improved understanding, because I do believe that the course which is being delivered is good, of what is required. Another thing which has happened, and certainly my inspectors have been encouraging it, is that in the bigger police forces, there is a danger, of course, because you have a great many superintendents, and any one may not have a high degree of expertise, so what you really want is you want a cadre of people who can be turned to who are authorised within the force to deal with applications for data, and that has happened, or it is happening.

Q709 ***Viscount Bledisloe:*** Is there a risk that this very good sounding instruction teaches people rather more what hoops they have to go through, rather than how they ought to be balancing proportionality?
Sir Paul Kennedy: I suppose that is always a possible criticism of any type of instruction, but I have no reason to think it is a valid one. Another thing I was conscious of is the form which they have to fill in, I know that it is easy to knock forms, but the form does provide prompts. The prompt does say, you know, is it proportional?

Q710 ***Lord Peston:*** As I understand it, traffic data is who talks to whom, it is not content, is that right?
Sir Paul Kennedy: There is a technical difference between communications data and traffic data, but I do not think that for present purposes is probably material, but data is who talks to whom; content is intercept.

Q711 ***Lord Peston:*** Then concentrating on traffic, one immediately thinks of telephones, but as an aside, you referred to actually looking at envelopes, does that actually happen?
Sir Paul Kennedy: Yes.

Q712 ***Lord Peston:*** Who writes to whom, and then there are e-mails.
Sir Paul Kennedy: Yes, I did not mention e-mails, but yes.

Q713 ***Lord Peston:*** As I understand it, within any organisation, if they wish to, as it were, apply, and I assume it is to you they apply for traffic data, they are supposed to consult senior people within that organisation as to whether they should do it, is that correct?
Sir Paul Kennedy: I am sorry, within a organisation?

Q714 ***Lord Peston:*** An application by an organisation for traffic data, as I understand it, before that application is made, whoever wants that is meant to ask a senior person within his organisation before they get to you as to whether we should be doing this, or something like that.
Sir Paul Kennedy: I am only looking at it retrospectively, like an audit function. This is what I said about, for instance, the operation of police superintendents. The Act and the Code of Practice provide that the authority to obtain it has to be obtained from a senior person within the organisation. In the case of the police, it is at superintendent level. In the case of the local authority, it is, for instance, the trading standards officer, it will not be a member of the trading standards department. It has to go up the tree to the correct executive level.

Q715 ***Lord Peston:*** I had understood that the purpose of getting that authority was as a protection for the ordinary citizen.
Sir Paul Kennedy: That is right.

Q716 ***Lord Peston:*** But surely the bias within the organisation will be the other way round. Why would a trading standards officer suddenly think, "I have to worry about the local people here", that is not the nature of their job, it is not the nature of their psychology, they do not go into being trading standards officers for that reason. Why would we assume remotely that this would give any protection to people?
Sir Paul Kennedy: First of all, as I said a little earlier, it is deliberately designed to be someone who is not involved in the particular inquiry which is then afoot, who is remote from it. I do not for one moment accept that they are not capable of saying, "Is this a proportionate operation? Is it necessary for the detection of crime?" Those seem to me to be things which senior members of local authority staff are quite capable of judging for themselves, and the proof of the pudding is very much in the eating.

When our inspectors go, they look at the files and they see why it was that an application for data was made by that particular authority, and in almost every case, even if they occasionally find that there have been procedural errors, their finding is that the application was justified.

Q717 ***Lord Peston:*** Sorry about this, to go back to my John Stuart Mill point, my view is that the person protecting the public should start from the position that this should not happen, and then the case has to be made overwhelmingly in specific examples. Is that your experience that the general view when you have looked at the paper trail, a typical thing is, "Oh, I do not think this, but convince me"; is that what you tend to see, rather than, "We are in the business of tracking people, the more the merrier"?
Sir Paul Kennedy: I think one has to adopt in a sense a realistic attitude to this. If you are in the process of investigating a crime, you will use such tools as are available, you will talk to people who may have been witnesses.

Q718 ***Lord Peston:*** Yes, of course.
Sir Paul Kennedy: One of the ways you can make an inquiry is to discover whether that particular mobile telephone was used to make a particular call. I do not have any difficulty about that, if it is necessary to progress the inquiry.

Q719 ***Lord Peston:*** I put it to you that to me at least, as an ordinary person, there is an enormous difference between looking for a witness who might have seen X shoot Y and looking at someone's private mail, it would seem to me to be on a totally different level philosophically.
Sir Paul Kennedy: Then you are getting immediately into the realms of what is the content, I was not talking about the content.

Q720 ***Lord Peston:*** But even merely knowing who I write to, what business is it of anybody to know who I write to, unless you have prima facie evidence that someone else has said, "He is a murderer, we had better find out who he is in touch with in order to" --
Sir Paul Kennedy: That may be the standpoint you arrive at, but it seems to me that if the police open the door of a house where they think there has been an offence of arson and there are a few letters on the doorstep, it would not be a bad idea to look at what you can discover from those.

Q721 ***Lord Peston:*** And you feel that that does protect the citizen?
Sir Paul Kennedy: I think we have taken great care to protect the citizen, because it has to be necessary for the purpose of the inquiry, it has to be proportionate, and it has to be authorised by someone who is independent from the inquiry, which is in fact afoot.

Q722 ***Lord Lyell of Markyate:*** It is really a follow-up point on Lord Peston to try and draw the line between what is and is not proportionate, and coming back to what you very helpfully told us about the need for serious crime, three years' imprisonment and so on. In a case where you ask for the telephone numbers on a mobile, or all a citizen's telephone systems, and you are trying to find out whether you know the number of potential drug dealers, and you look to see whether they are communicating with them, and obviously that will tell you a lot, I do not think anybody would object. But equally a computer would enable you to track down farmers who were suddenly buying a lot of fertiliser and maybe breaking the nitrogen rules; developers who were buying building materials at a time when you did not think they had got any permission to build; somebody with a cats' home buying a lot of cat food who may not have the necessary licence. Where would proportionality fall on those examples?
Sir Paul Kennedy: If you are the investigating officer, I would ask the question, is there any reason why you should not use the computer? I do not see any reason myself. It seems to me that you are entitled to do that. But you may not get it without going to the computer, I suppose, of the supplier of meal or whatever it is you wish to get.

Q723 ***Lord Lyell of Markyate:*** Will you not have to apply for a licence to see somebody's telephone records, and will they not say, an unlicensed cats' home -- I do not know if you even have licences for cats' homes, but an unlicensed cats' home, this is not the kind of thing that we expect this immense power to be used for, and no, you cannot have it. I would hope that would be the answer.
Sir Paul Kennedy: I think that is the answer in relation to the minor offences, I entirely agree, and the sort of things, as I said to you earlier, local authorities properly -- I think nobody has much trouble with the concept of the police using these powers, or not so much, but video surveillance was used by one local authority to capture a rogue trader who charged over the odds for shoddy work, and on one occasion charged a blind elderly lady £700 to cut her lawn, and then frogmarched her to a cashpoint to get money. If you can use any form of enquiry which detects who did that, why not? I have no difficulty with this. What I am concerned about is that the tools given should be properly used. Parliament has decided the tools can be given.

Q724 ***Baroness O'Cathain:*** In your report, you say that weaknesses and errors were found by the inspectors in a significant number of cases. Can you

elaborate on these deficiencies in compliance with the laws and codes? Actually, are the laws and codes now relevant because of the advance of technology, should they not be looked at every year and tweaked?
Sir Paul Kennedy: The Code of Practice in relation to data in particular is more or less hot off the press. No, that is the other one, but it is only formally completed this year. I accept that they may have to be looked at as time goes on, and one of the developments, of course, is that the mode of carrying telephone communications is changing rapidly to internet, and all of that kind of thing will involve some changes. But so far as weaknesses and errors are concerned, most of the errors in the past have been procedural: transposing numbers, where one person gives a number to somebody else and they write down the digits in the wrong order. Fortunately, what has happened to some extent is that increasing use of the machinery that is available means you cut out the human element, but if you put in the wrong number in the first place, it will still go through the machine. They have now divided errors into reportable errors and recordable errors, and that is good. Reportable errors in broad terms is where information is obtained as a result of the error which should not have been obtained; recordable errors are errors which are simply recorded within the organisation, but have to be produced to my inspectors when they go, which is useful, because you can see whether they have been making mistakes, but we do not have to have a correspondence about an error which has not actually produced any material. Now early on, there were errors of this kind, and I mentioned earlier on the importance of the designated person in the process, that the senior point of contact in some police force services would draft the remarks for the designated person to insert in the appropriate box. We take the view that is wholly wrong, that the independence which is important should be demonstrable. That kind of thing did happen; it does not, as far as we can now see, happen at all, but it was lack of familiarity with the process and an attempt on some junior officer's part to support his senior by giving the information he thought they would require. Within local authorities, one can get the difficulty that they do not realise this does not help very much, but that there needs to be a wholly independent mind, and therefore the trading standards officer gives permission in relation to a trading standards inquiry, that is the sort of thing we have been talking about. What we have not found, and I can say this with complete confidence, is any evidence of bad faith. That would cause real concern; "This inquiry should never have been made", that simply has not arisen. Sometimes, the justification for it is not well expressed, but when you dig deeper, yes, there was good justification for it. I hope that that answers the question in general. What I would have liked to have thought is that after the first round of inspections, things would be so much better, and you would not actually need a second round. Unfortunately, life is not quite like that, and what happens is that people change, key officers change and so forth. We have found on second inspections rarely that there has been a bit of slippage, and things are not quite as good as they were. Conversely, we have found remarkable evidence of improvement, but I do, I am afraid, accept a premise which I was more reluctant to accept initially that we do need to inspect and go on inspecting in order to maintain the standards, but what we do, and certainly the inspectors do, is if you get a really good inspection, you say, "We will come back in 18 months", whereas if you get a bad one, "We will try and come back in six months".

Q725 ***Baroness O'Cathain:*** Can I just ask, do you have an analysis, not for us, but in your organisation, of the errors to see if there is a trend in repeatable errors, not necessarily in the same area, not in the same police force or wherever, but so that you could then change your training programmes or your suggestions for training programmes to put more importance on those areas which seem to throw up more weaknesses?
Sir Paul Kennedy: We certainly know what the errors are which happen frequently, yes. I would not trouble you with them, but every inspection -- curiously, not my inspections, because mine are fewer in number, but all of the inspections of police forces, for example, lead to a report of something of the order of 20-30 pages, around 20 pages, and I read them all, so in fact, I do see what the errors are, and my inspectors read them all too, because they generally, most of them -- and we do have meetings of inspectors where we discuss what is appearing to be a difficulty, and there are lines of communication which enable us to pass that back to those who are training, yes.

Q726 ***Baroness Quin:*** Before I ask my question, could I just follow up on what Lady O'Cathain said about errors? You say in paragraph 55 of the report that no errors were reported by the Home Office, Scottish Executive, Ministry of Defence, SIS and so on. As much as I respect these great organisations, is it credible that they do not have any errors at all, and can you give them a clean bill of health in this area?
Sir Paul Kennedy: Yes, the short answer is yes, but it is only because they are highly professional in their own operations, and what we are concerned about is whether a warrant was granted when it should not have been granted. By the time it gets in front of the Secretary of State, it should not be in a condition where in fact it discloses an error detectable by me on inspection. I would be very disappointed if we had a

lot of them. The odd one, yes, but anything more than an odd one would be a problem.

Q727 ***Baroness Quin:*** Thank you. My question is: do you think that the Investigatory Powers Tribunal's role is too limited by its inability to investigate interceptions that were not authorised by warrants, and do you think that citizens' rights are adversely affected by this constraint?
Sir Paul Kennedy: In a sense, this is really a question for Lord Justice Mummery, because I do not have any overall view of even what the Investigatory Powers Tribunal's workload is. It sounds, in a sense, surprising, but for obvious reasons in this area, nobody tells you what you do not need to know, so I know when they impinge upon that which is my concern, but not in other areas. I do not see that, as I understand it, they have no role to play, and I did make enquiries in relation to this question, in relation to any complaint which does not identify one of the organisations within the statute as being responsible for the irregularity. In other words, if someone comes along and says, "The police have been bugging me and they should not have done", then the Investigatory Powers Tribunal will look into it and take action in relation to it. If they come along and say, "I have been intercepted but I have no idea by whom", they will say, "We cannot help you". But this is really partly because of what we were talking about earlier, that if they had been illegally intercepted by somebody without a warrant, it is really a matter for the police and not for the Investigatory Powers Tribunal, and they do not actually have the facilities to deal with that, because they have no investigatory staff of their own; in order to make the investigation, they go to the authority which is alleged to have abused its power and make enquiries. I do not think that any change in the position would work without creating an enormous investigatory staff for them, and then it would change the nature of the Tribunal.

Q728 ***Lord Rowlands:*** In your annual report, you referred to your participation in an international conference called "Balancing National Security and Constitutional Principles within a Democracy". Did you come back from that conference with any thoughts about safeguards that other nations are using or any aspects of good practice that we ought to sort of think about adopting?
Sir Paul Kennedy: I think it is very useful, because you do see people who are dealing with these problems. One of the things I certainly came back with is an increased knowledge of the way in which they use judicial oversight. I think sometimes, on most people, they have different frontiers between different functions. We talked about that earlier, whether Sir Christopher's role and mine should be different, and if so, where the line should be drawn. I do not say that I have come back with any idea I burningly want to see changed here now, because I think they do it better than we do, but obviously it is one of the things you do look for and hope to gain from going.

Q729 ***Lord Rowlands:*** But you did not find any in this particular case?
Sir Paul Kennedy: There is no magic bullet.

Q730 ***Lord Lyell of Markyate:*** At paragraph 61, you talk about the debate about whether intercept evidence should be used in court, and you say: "I am firmly of the opinion that the benefits of any change in the law are heavily outweighed by the disadvantages, and with one exception, everyone to whom I have spoken in the course of my visits seems to be of the same opinion." This is obviously a very important and hot debate at the moment. Could you expand a bit on the fundamental reasons why you take the firm opinion that you do?
Sir Paul Kennedy: I may say that the recommendation which has been made, and which I had the advantage of being asked to give evidence in relation to that Committee about, is one that I am sure will be cautiously and carefully brought into effect, if that is what Parliament so decides. But I am told and accept that the danger is that if you start to use the material in evidence in court, you will far too quickly disclose the means by which you carry out this kind of activity in a way which will be of serious assistance to those who wish to engage in illegality. It is not only in simple terms what we can do and how we do it, but it is what we cannot do, and there are serious areas which we cannot cover, and there are a lot of people who would like to know what they are. The nature of English criminal procedure being such as to require a high degree of disclosure, it would make it very difficult to comply with our normal criminal requirements for disclosure in a way which was technically safe, so far as security services are concerned. That is really what it amounts to.

Q731 ***Viscount Bledisloe:*** Because it will be for the prosecuting authority to decide whether or not to wish to use this evidence. If they feel that the danger of using any particular item of evidence or any particular witness is of the kind that you have spoken about, they decide not to do it, but why should such evidence not be admissible at the wish of the prosecution if they feel that risk does not exist or is minimal?
Sir Paul Kennedy: It may be possible to go down that route, but if they decide to use it, there is no question that the defence will say, "You have only shown us part of the picture, let us see the rest", and they are entitled to ask the question, and it then becomes a

matter for the judge in the individual case to decide how it is going to be answered.

Q732 ***Viscount Bledisloe:*** Except if you are going to make it admissible, you limit the terms of what can be explored.

Sir Paul Kennedy: Well then, you come up against the difficulty in Europe, do you then have a fair trial, where only the prosecution can produce -- that is the argument, that is the difficulty.

Chairman: Sir Paul, you have been extremely generous with your time, can I thank you very much indeed for joining us, and indeed for your evidence.

WEDNESDAY 4 JUNE 2008

Present
Bledisloe, V
Goodlad, L (Chairman)
Lyell of Markyate, L
Morris of Aberavon, L
Norton of Louth, L
O'Cathain, B
Peston, L
Quin, B
Rodgers of Quarry Bank, L
Rowlands, L
Woolf, L

Examination of Witnesses

Witnesses: PROFESSOR DAWN OLIVER, Professor of Constitutional Law, UCL, and PROFESSOR JÖRG FEDTKE, Faculty of Laws, UCL, on the Surveillance Inquiry, examined.

Q733 ***Chairman:*** Can I welcome you both to the Committee and thank you very much for coming. We are being recorded but not televised so could I ask you, for the record, to identify yourselves. If you would like to make a short opening statement, please do so; if not, we will go straight to discussion.
Professor Oliver: I am Professor Dawn Oliver. I am Emeritus Professor at the University College London and my speciality is constitutional law. I do not have an opening statement.
Professor Fedtke: I am Jörg Fedtke. I am Professor of Law at University College London. My speciality is constitutional law in comparative perspectives.

Q734 ***Chairman:*** Perhaps I could start by asking if you think there are any existing constitutional conventions or principles that are threatened by the spread of surveillance and data collection and if you think any limits should be imposed on the state's powers in those sort of areas?
Professor Oliver: I think it is very difficult to identify existing constitutional conventions or principles. Of course we have the Human Rights Act and we have the Data Protection Act, both of which, I would say, express constitutional principles to do with protection of dignity, autonomy, privacy and so on. It is very difficult to be precise about what limits there should be on the use of data protection in the possession of government. I myself am very concerned about data sharing and the extent to which different government departments or state bodies are entitled to share or transfer information they have in one capacity to another part of government. I also feel there need to be statutory provisions about the extent to which government bodies are entitled to retain and use information that might have been obtained not under statutory powers but just accidentally or because information is around. The basic legal position normally is that the Crown and other non-statutory bodies have the same freedoms as ordinary individuals. That came out of the Malone case which you probably know about. My concern would be that there need to be statutory provisions indicating what can be done with information that has been acquired in those ways.
Professor Fedtke: Professor Oliver quite rightly emphasised the importance of the Human Rights Act and the right to private and family life. I would perhaps add a comparative slant and say that the right to control your own personal data is, in some countries, regarded as a human right in its own right beyond the general right to privacy. The right to know who knows what about you at a particular point in time is, for instance, identified as a constitutional right by interpretation of the German Constitutional Court in that country. Much of this is actually, as Professor Oliver emphasised, encapsulated in the Data Protection Act and its principles, but that is on a lower level and is an ordinary act rather than a constitutional principle. I would argue that the right to control one's own data in this day and age comes close to a human right. I would also add, as far as constitutional principles are concerned, the right to judicial review. If you look at some statutes dealing with surveillance or data protection, the question arises what is the role of the courts. Personally I would rank that as a constitutional right, a right to have access to a judicial forum to review whatever measures were taken by the executive and that triggers one or two questions. If you look at UK legislation, is the individual who is affected by surveillance informed after the end of a particular measure which in turn allows him possibly to access the courts to raise a case? In many of the statutes in this country that right is not given but in other countries that right is prescribed on each and every occasion. The right of individuals to actually be informed of particular measures is very important. The involvement of the courts in the authorisation of surveillance, in my view, comes close to a constitutional right and has to do with the division of powers between the legislature and the judiciary. I think that other countries may have gone down different avenues, for whatever reasons, in that they require judges to authorise particular instances of surveillance and I would add that to the more general right of privacy and family life which we find in the

Human Rights Act. In terms of limitations, and I will try to cut myself short here, again I would stress the importance of very detailed authorisations in statutes. Is there a proper authorisation that sets out in great detail what public authorities may do when it comes to surveillance and data protection? Are there internal safeguards against abuse? I think that is an important element as well. Are there Chinese walls between different government authorities when it comes to the sharing of data? All of these questions relate to the limits of what the state may do in this area. Finally, is there an absolute core of privacy which is absolutely protected from any intrusion or any surveillance? Other systems do recognise that there may be such a core, although again I would stress here that it is very difficult probably to define what that core, in essence, is. These are the limits to what the state should be doing in this area.

Q735 ***Lord Lyell of Markyate:*** That is an extremely interesting list. The distinction between overt and covert seems to me to be very important. There are complaints, for example, that local authorities are using covert powers where really the justification should be overt. A very simple example is dog fouling. I think it is a good thing to stop dog fouling but they should know if there are cameras being used and there should be signs saying so, which would probably be rather effective anyway. That is not constitutionally protected, is it, and would require statute?
Professor Fedtke: It would require statute. I agree entirely with your observation that the principle of trying to obtain data with the person who is actually affected, perhaps the dog owner or the parents of children who send their children possibly to school in the wrong catchment area, the principle that public authorities should first and foremost act openly and first and foremost address or approach the person they are dealing with or the person who is in the focus of their activities, is a thing which should be put down in the statutes. If you look at the German Data Protection Act that is one of the first things you find. Public authorities should target the individual who is involved in the proceedings and do so openly and try to obtain as much information as possible on that basis and only then can other measures perhaps be contemplated if the public authorities need further information.

Q736 ***Lord Peston:*** My question somewhat anticipates what I meant to ask you but this is an ideal place to put it. You referred to a protected area at the end of your first statement. Certainly when we were students we were taught about John Stuart Mill on this, and if I may quote his exact words*: "There is a circle around every individual human being which no government, be it that of one of a few or of the many, ought to be permitted to overstep."* He says the point to be determined is where the limits should be placed but he had no doubt whatsoever that there should be such a limit. We did have here a judge last week who was meant to be supervising exactly this kind of surveillance and when I put that question to him he pretty well said, which worried me enormously, that the philosophy of John Stuart Mill is now dead. Some of us do not think it is dead; quite the contrary it is what we believe in more than almost anything. I would like to know your view on the matter.
Professor Fedtke: I indicated that I do believe there could be such a core which should be absolutely protected. We may come back to that later on when it comes to specific statutes and the way the state goes about regulating surveillance and data protection. That is just a footnote at this point and I might be able to elaborate later on. I very much believe in detailed specific statutes rather than general provisions which cover ever so many public authorities but that is a different question. In Germany the highest level of possible intrusion, surveillance, wire tapping and so on, actually excludes judges from authorising measures and gives this authority to parliament. In that statute, which in Germany is the highest level of possible intrusion and which contains the highest level of safeguards as a counterbalance, you will find provision which says under no circumstances may the core of private life, if surveillance focuses solely on that, be infringed. Not even on that very high level is there absolute access. There is a core which is difficult to define and that is the main problem here.

Q737 ***Baroness Quin:*** I am interested in what you were saying about the position in Germany. Have there been changes in Germany as a result of the worry about terrorism which has somehow gone against the general trend in that country?
Professor Fedtke: Perhaps one introductory remark. I am German so my legal education and my PhD thesis were in that jurisdiction which is why I am particularly interested here in that country. There is a second reason why Germany might be a good system to look at. Germany enacted worldwide the first Data Protection Act in 1970 even before the United States. It is a system which has grappled, for a fair amount of time and to the present day, with these constitutional court decisions in that particular area. It is a long story. To come back to your question concerning changes in the approach and the impact of terrorism, Germany is interesting because in the late 1970s it experienced a serious threat of terrorism. You may recall the hijacking of a Lufthansa aircraft to Mogadishu and the killing of the pilot and then the intervention of German security forces. In that context you have appearing a number of quite severe statutes which enabled the state to react to such pressures. Yet, at the same time, I do sense that there has been a balance. To the present day measures which

have increased the ability of public authorities and security services to monitor particular activities have been counter-balanced with procedural safeguards, in particular the involvement of the courts with information even on that high level of individuals affected by surveillance once the measure has been completed, which again triggers the ability to access the courts and to apply for judicial review. I think that Germany has a very, very early system when it comes to data protection. It has experienced quite a severe terrorist threat. It has not immediately succumbed to changing the legislation and allowing security forces inappropriately high access or rights or powers because there was a fair amount of counter-balance. We might want to look at those elements later on in the discussion. It is a continuous battle and even to the present day the Ministry of the Interior is trying, at every corner, to increase the powers especially of security forces. Basically it is a struggle between those in favour of liberty, of freedom of data protection, and those who argue very strongly in favour of the state, public interest and security and safety.

Q738 ***Lord Morris of Aberavon:*** On the principle of overt as opposed to covert, particularly on the instance given as an example by Lord Lyell, are there not limitations on that which undermine the efficiency and the need to observe? A policeman does not give away the point that he is observing a drug pusher from across the road. The defence may demand it and the judge then has to reach a decision. If he is adverse to the Crown then the Crown frequently withdraw the case. We enjoy the sign that there are cameras for road speeding but we do not have cameras for going into a bus lane. Are there not limitations on that or does it not depend on the personality of the observer? Are the police in a special position as opposed to the Council looking at dog fouling or children going to school in the wrong areas?
Professor Fedtke: I agree data protection, if taken seriously, is one of the greatest challenges of public administration simply because it is very difficult to develop a workable balance between the data protection, on the one hand, and a very onerous system of checks and balances, of internal Chinese walls and limitations. It is very difficult to balance these two. I would agree that it is a question of the case at hand. The policeman watching someone from across the street would be able to do so in Germany without much limitation despite the existence of a fairly elaborate data protection regime. If the policeman was to use some form of device which enables him to listen in across the street then the whole scenario changes and you would have a special statute which would authorise that or set limits on it. The distinction between overt and covert surveillance is a difficult one to draw on itself, which again begs the question how do public authorities deal with that. It is an investment of time and energy to have people who actually take that decision and say this is on this side of the line and that crosses the border.

Q739 ***Lord Rowlands:*** Do I infer correctly from what you have been telling us that you do not find it attractive the way we have gone down the route of these commissioners, the information commissioner and the surveillance commissioner, and that is a less effective route than the one followed in Germany? Are you making a direct comparison between the two and are you critical of the commissioner route as it were?
Professor Fedtke: The commissioner route is the right one; there is no doubt about that. Germany has a data protection commissioner on a federal level and on the state level. There is a team of 17 commissioners who have been very influential in securing data protection on a very day-to-day basis. If you look at the development of data protection, in particular in Germany, combined with surveillance, you will see that the impetus for legislative performance frequently comes from commissioners who have been working in this area and who compile and watch developments very closely. I am all for commissioners but the question is what are the powers of these commissioners. Are they used to authorise certain measures or are they only used to supervise certain areas *ex post facto* when things have already happened? What is their ability to investigate particular instances of surveillance or the use of data? I am all for commissioners but the question is what powers are attached to them.

Q740 ***Lord Rowlands:*** The German commissioners, are they privacy commissioners? We went to Canada and heard that they divide privacy from freedom of information whereas our Information Commissioner does both. The argument we had in Canada was there was a potential conflict of interest between the two. In the German model are there privacy commissioners or freedom of information commissioners?
Professor Fedtke: Here I would say that the English system is very much advanced compared to the German when it comes to freedom of information. In that area the Germans are struggling to catch up with the United Kingdom. Access to information is something which this country has championed and where the Germans have done very badly. I think the two in Germany are seen as separate entities although there is a big mix. If you look at the Data Protection Act in Germany as well as in this country, there are rights to access data so obviously the two are very closely intertwined.

Q741 ***Lord Rowlands:*** You would prefer a model where they are separate.

Professor Fedtke: Both are very closely related. I would not really have a strong opinion either way as there are advantages and disadvantages in both. The development has been quite different and I could not even say why. It is remarkable that this country has developed access to information very well and Germany has neglected it. Germany has gone quite far ahead in terms of data protection whereas this country might have some catching up to do there.

Q742 ***Baroness O'Cathain:*** We move now from the constitutional conventions or principles to constitutional relationships. Professor Oliver, what do you feel about the relationships between citizens and the state and how they have been affected by the increased use of surveillance? How are they likely to be affected with the inextricable march of better technologies to do just that? Do you believe that they are a threat to the constitutionally established understandings of citizenship in the UK?
Professor Oliver: A difficulty is we do not have a very articulated understanding of citizenship. For me a major problem is the risk that individuals will feel that they cannot trust the state with the information that it has about them and that might make them feel insecure and unwilling to co-operate with the state, unwilling to provide information, for example about their tax and so on, because they are concerned it might be either lost or get into hands they do not want the information to get into. For me the main thing is this question of security, trust and co-operation. Our system depends very largely on law abiding citizens being willing to co-operate with the state and do their tax returns and generally do what is required of them. I find it difficult to be more precise than that about the effect of this information.

Q743 ***Baroness O'Cathain:*** I suppose your comments are a direct result of all the CDs and data that has gone missing. Would there be a reason to have regulation to make sure that any data should be encrypted straight away once it is used just in case it falls into the wrong hands?
Professor Oliver: It sounds a good idea. I do not really understand what can be done to data to protect it but I cannot see an objection to it myself.

Q744 ***Baroness O'Cathain:*** It does seem strange that more data can go all around the country and fall into all sorts of wrong hands without being encrypted. The last thing we want is more and more laws but do you think it is something to consider?
Professor Oliver: It might well be and I am sorry I cannot say anything very strong about it. One of the problems is we think about these matters on the assumption that our public servants are honest and incorrupt, which fortunately they are, but of course as it becomes known that public servants might have access to information that would be valuable to criminals they are likely to be targeted. We have to get our heads around a scenario that you might not be able to trust, as we do, public servants. I am not quite sure how to deal with it.

Q745 ***Lord Peston:*** We have surveillance and it arises essentially from the question of security, both individual security and national security. I do not think any of us doubt that is something we have to take very seriously. The real point, it seems to me, is the limits point which has been raised by both of you. You could put it another way around: if you give any authority any power, and it is not to do with corruption, they will test that power to the limit. Certainly we have had some rather horrific evidence. The most amusing of all was a professor who came to us and sat in the Square and his stuff was searched under the anti-terrorism law. He was just sitting there because he was early before coming to give evidence. I find it hard to believe that parliament enacted that legislation so professors, of all people, should be searched. It is a not a question of professors but can we draw the line somewhere, and in particular whether the human rights thing protects us in practice in the relevant way?
Professor Fedtke: In the light of the German experience, human rights have provided a very good shield, a very good protection. As you rightly say, the difficulty is to strike a balance between the national interest and security and safety for the people and the interest of the individual to be protected from excessive surveillance or an excessive use of data. I think that the Human Rights Act and the European Convention on Human Rights have had a positive impact in this country as well. Legislation has been put into effect in order to regulate surveillance and data protection under the influence of the European Convention on Human Rights or other measures: international laws such as the Data Protection Directive of the European Union. I do think that human rights provide a strong bulwark but then you have to zoom in and look at the details. I am afraid a general right to privacy is difficult to put into practice and it needs teeth. There I would strongly endorse specifically legislation which deals with particular areas, particular activities of public authorities, and balances very carefully what these public authorities need in terms of information and what they can pass on for the exercise of their particular duties and the right of the individual to be protected from excessive surveillance and data mining.

Q746 ***Lord Peston:*** In terms of viewing it in terms of legislation, and I well understand the spirit in which you are making those remarks, there is often difficulty writing into legislation the way you want it used. To take an obvious philosophical point which refers to

the balancing question, you could say we are passing this legislation but we want it used in the last resort and only when you have to. Compare that with we are passing it and use it in the first resort. Many of us in this area take the last resort view. The great row going on about the 42 days now is the danger that it will become the normal thing rather than the thing only *in extremis.* Are you optimistic that if we go down the line of balancing that parliaments of different sorts can persuade the people who are doing the actions that many of these powers, because security is so important, should only be used as a last resort? To give you another example which absolutely horrifies me, I gather the City of London uses what powers it has to clock every car going through the City of London. The idea that the City of London should have the power to clock every car going in and out, which I gather they do on security grounds, to go back to my John Stuart Mill point as an old-fashioned liberal, I just find it not a world I would like to live in. That they should be able to use those powers in the last resort is another matter. What is your response to that? How can we as parliamentarians get the last resort idea into our legislation?

Professor Oliver: That is difficult. The fact of the matter is it is not just the City of London because there is the congestion charge. Interestingly I do not think when the congestion charge was being introduced anybody was worrying about the fact that it would mean your car number was taken. To home in on the point, it is very difficult for parliament to spell things out. Of course, holding bodies accountable, getting them to report on how they have used their powers and then investigating it, is one matter. Another possibility, for example for the police force, might be for them to articulate their policy. Re the professor who was searched outside parliament: maybe there is a police policy that anyone with a rucksack or a briefcase within X yards of parliament should have that brief case searched. I can understand that; but it would help if some of those rules were published so that people knew that you should not sit in Parliament Square with a briefcase if you do not want it searched. Also people can then say "that is excessive" or "you should do more". The policy behind the exercise of some of these powers, in some circumstances, could be more open.

Professor Fedtke: It is a question perhaps of definition. If you want to protect national security, how do you define that? It is very difficult for parliament in any system to come to grips with that problem. I find that the use of very general terms, and national security could be one example, is problematic. How do you solve that? You could introduce in legislation a list of criminal offences which endanger national security so you are giving flesh to the term as a legislator. You are telling the public authorities national interest is important, that is a value and will justify quite severe measures but we define that term as follows. Then you can have, in some systems, quite elaborate catalogues of criminal offences which give flesh to what is intended. That is what you are supposed to do. On the plus side, the principle of proportionality has entered into legislation in this country and that requires public authorities, not in each and every case but in most cases, to check whether there are milder means. Milder means that is an indicator, that is the flashlight, it is the last resort, look around to what you can do before you actually use this tool. That is a very valuable method of approaching that particular problem. I keep on repeating myself on this one point, that the task for parliament becomes easier if you regulate specific areas: local authorities with their powers and their surveillance methods which need certain requirements, conditions need to be met; then health authorities; then an authority dealing with identity cards; the police and security authorities. That is a lot of work but if parliament shapes the conditions for each and every case then I think you come closer to achieving your aim.

Q747 ***Viscount Bledisloe:*** The last answer goes some way to answering my question. I was concerned about proportionality, not only to question whether it is a last resort but whether the crime you are seeking to discover about merits the level of scrutiny. I am thinking in particular of the powers given under the Prevention of Terrorism Act being used to discover whether the right child is going to the right school or the right dog is doing its business in the right place or all these minor things. Do you think this should be regulated by much more detailed statutes directed to particular authorities or an alternative method that you have a specific proportionality commissioner? We have heard from the information commissioner, and so on, but they tend to take into account whether the question of proportionality was considered but not whether the decision was right. Do we not need someone, maybe parliament, maybe not, to say this sort of power should not be used for this sort of much lesser conduct?

Professor Oliver: That is a very interesting point and I have not come across the idea of a proportionality commissioner before.

Q748 ***Viscount Bledisloe:*** It came to me about ten minutes ago.

Professor Fedtke: The principle of proportionality in Germany is a constitutional principle and ranks side by side with human rights. It is one of the top elements which public authorities need to take into account in exercising their powers, whether surveillance, whether it is dealing with personal data, or whether it is any other function they might perform. I would hope, in a human rights culture, that step by step every public official dealing with these types of scenarios will have

that idea in mind: my actions need to be proportionate to the aims. If you link particular activities, measures or powers to the controlling device of judges, as is very usual in other systems, you will have someone like a proportionality commissioner in the guise of the judge who will look at the measure, the information the public authority has, the aim it is trying to achieve, the personal circumstances of the individual affected and will balance these elements and either authorise it or withhold authorisation. In a way, that is perhaps good.

Q749 ***Viscount Bledisloe:*** My concern is if you leave it to the individual in question, if you are the school attendance officer and it may be the last resort for finding out about the school attendance, and you resort to these measures you are not going to be the person to say that school attendance is not sufficiently important to use this sort of activity; you need an outsider.
Professor Oliver: One body that might be able to deal with these questions would be the ombudsman, either the parliamentary ombudsman or the local government ombudsman. If someone is complaining that a local authority is using surveillance to see if they are sending their child to the wrong school, then they can complain.

Q750 ***Viscount Bledisloe:*** By definition they probably will not know it is happening. It needs some affirmative person saying you cannot do this and not someone dealing with the occasional person who finds out and complains, is that not right?
Professor Oliver: You are right. It would not cover everything.
Professor Fedtke: Internal safeguards might be of help. I mentioned the top level in terms of intrusion in Germany. Those measures which affect the existence of the nation or a particular province, very substantial threats to the structure of the state such as terrorism, could fall into that if it is directed at eliminating or substantially hampering the existence of the state. Measures are authorised under that Act. Parliament exercises directly the power to authorise them to go ahead or not, but then internally the authority which actually takes action has to ensure that there is someone who supervises each and every piece of the enfolding story, of surveillance for example, who has the training to be a judge in Germany, which means a lawyer with specific legal qualifications. That is an internal mechanism. I think much of the discussion neglects the fact that public authorities themselves should be the first instance of protection. They should have internal mechanisms which safeguard in themselves the protection of the limits or adherence to the limits. That is an interesting example where you would not have the policeman who would then go off with authority but you would have someone supervising him because it is a measure which has a high intensity. You need someone with a legal qualification not just to review it and sign it off but to go along on each and every step and to say if this is OK.

Q751 ***Lord Lyell of Markyate:*** You say someone with a legal qualification but we have this system of magistrates, 28,000 ordinary people reasonably trained, and in a way we look to them to do what is proportionate when it comes to penalty. You remember the dust bin case up in Cumbria. I thought the magistrates were entirely right to confirm that the penalty should be there but I rather questioned whether it was proportionate to have doubled it. Comment in the press and that sort of thing would, if we leave quite a lot to the courts and the magistrates, cause that to settle down.
Professor Fedtke: The magistrates would be in a good position to add a further element of control in this area. I agree entirely with that.

Q752 ***Lord Rowlands:*** I am puzzled and I come back to the point. You said the judges would be the judge of proportionality but what do the German commissioners do? Why are they not the judges of proportionality?
Professor Fedtke: Data officers and data protection commissioners can be approached by citizens who feel that their rights have been infringed and they then have investigative powers.

Q753 ***Lord Rowlands:*** Why go to a judge if that is the role of the commissioner?
Professor Fedtke: The point is that the commissioner does not authorise surveillance activity. He is not the person who would strike the balance, look at the case or give the go ahead to the public authority but it would be the judge who would have to sign off the measure on the basis of the information provided to him by the public authority.

Q754 ***Lord Woolf:*** I was interested in your combination of proportionality and specific legislation dealing with details of what you can and cannot do. If you are going to apply a proportionality test, then is not the idea of having specific legislation which says what you can and cannot do curtailed by the specific legislation so, in fact, what you are saying has an internal inconsistency?
Professor Fedtke: With due respect, I would probably say the opposite may be true. Having a set of laws which starts off on a general basis allowing the policeman to observe things on the street without rushing off to the judge and ending with a law which actually circumvents the judge and says parliament itself will authorise this, is problematic. To have a set of statutes which determine or are designed to cater to different levels of intrusion is in itself an element of

proportionality. You deal with the lesser intrusions in a specific statute, allowing perhaps more public authorities to draw on that authorisation, and the stronger the infringement, the stronger the limitation of a human right, the more specific is your legislation which tries to strike the balance between the right, which is more effective than in the first scenario, and the interest of the state in acquiring information which has to be weightier.

Q755 ***Lord Woolf:*** I will press you a little further on this. It is very interesting and I think it is partly a cultural distinction between the German approach and our approach which explains why in Germany you have many more judges than we have in this country. It is important because certainly as a former judge, and still a judge in some ways, I found that one of the great weaknesses of the Data Protection Act is there was such a mass of detail in the legislation that nobody, not even the judges unless they were very specialist—the professors were very specialist but most judges were not specialists—cannot comprehend the legislation. If you are not careful, if you go into too specific detail, you are going to have the dust bin example. Especially if you are applying principles of proportionality, it is very difficult to anticipate all the circumstances. Would you at least agree with me to this extent that probably a very good way of going forward is to start off with general principles, then have a commissioner or some other person who supervises and oversees it in practice, and only when have you a very substantial experience do you go into legislation if you are entitled to do that? I know from actual data that we were falling very far behind and so we had to make a leap forward. There are dangers in that and for a general policy you want to be very cautious in rushing into legislation.
Professor Fedtke: I agree with most of what you have said, the first point being interesting: the number of judges. A system which has so many judges can deploy them to give authorisations. If you are limited in the number of judges then that becomes a resource problem. I agree entirely. In terms of general principles, a data protection commissioner to supervise developments and to flag when things go wrong is entirely accepted and then to move into more detailed legislation when you identify particular areas which merit more detail. Again there is the question where do you draw the line between the general statutes and where do you cross the border to the need for a specific one. The Data Protection Act is very complex; I agree entirely. Reading and working with it is horrendous. Perhaps the answer to that is it tries to cover so many instances it gets very abstract. If you have a specific statute, if you look at the code of criminal procedure in Germany, if you look at the specific laws on the state level, meaning the regional level, which deal with surveillance and data protection or the use of data by police authorities, you will read them and you will understand them immediately because the measures are described in pure normal language.

Q756 ***Lord Woolf:*** Is there not a danger of a conflict between the different legislation? There are all sorts of areas of demarcation so which legislation do you use? I was going to suggest to you that in the area we are talking about there is lot to be said for an holistic approach. I would not necessarily share the Canadian idea. There are two different principles here and it is always going to be a balancing act between two principles.
Professor Fedtke: Again I agree. Let us go back to the Data Protection Act which exists in Germany and which exists in this country. The Data Protection Act in Germany is the foundation for all public authorities. All public authorities are inevitably bound by the Data Protection Act; there are no exemptions. The system then goes on to say if you have specific legislation that may, if it is so prescribed, qualify the general application of the Data Protection Act. The higher you work yourself up in the hierarchy of laws you will find more specific information about what particular authorities can do, but the Data Protection Act, as such, is very broad and covers everything. In the United Kingdom you have a number of exemptions which are quite substantial. They are difficult to define and I think they make the whole matter much more complex than perhaps with a different approach relying more on specific legislation.

Q757 ***Lord Morris of Aberavon:*** What body do you believe would be best placed to protect the constitutional rights of citizens against over-zealous surveillance and data collection? You have the options of parliament, the courts, some other body, but is not the basic problem what information or knowledge they have in order to act as some kind of policeman? Within memory we have had allegations against MI5, evidence given about being economic with the truth, fears, warranted or unwarranted, by people from the prime minister down about surveillance. How can you get parliament or a judge to be informed so he can take the protective view of the citizen?
Professor Oliver: There could be a new official called perhaps not the proportionality commissioner but a protection from surveillance commissioner who would be concerned partly with general policy issues, in other words to take a broad overview of what is happening. If people are particularly worried about dog fouling, this commissioner could look into that and then report to parliament, and obviously to the public, providing some actual factual information to inform people's comments about it. That approach

might help. That person might be an officer of parliament or an independent commission with that remit. They would overlap quite a lot with the Equality Commission but we can live with overlaps. That might be an institutional arrangement which would provide parliament and other bodies with the background information they need to engage with the problem.

Q758 ***Lord Morris of Aberavon:*** How can he be assured that he has the necessary information? You may appoint the body but how does he know what is happening?
Professor Oliver: He might be given powers of access, the right to demand information from the bodies he is investigating.

Q759 ***Lord Lyell of Markyate:*** Two of the ways that we deal with it at the moment are you cannot necessarily stop it beforehand, and obviously a commissioner cannot be looking at everything all the time, but when it comes to be used you make the evidence inadmissible and when they try to use it when they should have never been doing it some penalty could fall into place. Are not those two pretty practical protections?
Professor Oliver: Used appropriately, yes. I myself would be a little concerned about a serious terrorism trial collapsing because information that was extremely relevant had not been properly obtained. There is a big debate there I know. A subtle approach to these problems from various angles would be very helpful. For example, as you are suggesting, to discipline police officers or whoever who have overstepped the marks, making it quite clear where the bounds of their authority are, would be one helpful approach. Elaborating codes or standards for certain organisations as well would be another way because at least then the officials know what they can and cannot do or whether they are somewhere on the edge and that gives a peg on which to hang criticism of them.
Lord Lyell of Markyate: Your first point, which I agree with, is that a trial should not necessarily completely collapse. The courts have indicated sometimes that improperly obtained evidence can be admitted but at least the fact that it was improperly obtained comes into the public domain and might be dealt with through one of the other routes.

Q760 ***Lord Norton of Louth:*** What role do you think parliament should play in this? Is their more of a role that it should take on? There have been criticisms that perhaps it is too willing to go along with government demanding more surveillance powers and so on. I think you are implying in Germany that the legislature is more active in this sphere. Is there a role that parliament should be playing that it is not playing?
Professor Fedtke: The role of parliament is predominantly to legislate and the detail of legislation, which we have talked about this morning on various occasions, is a task for parliament to apply its mind to and to try, in my personal opinion, to draft the statutes which authorise surveillance and the use of data in very specific terms. That, in itself, is a formidable task for parliament and is very difficult to do. There are data protection commissioners who report to parliament. These reports should be taken seriously and should be as elaborate as possible because that is one source of knowledge for parliament to actually see what is going on. It is an independent commissioner after all with powers to ask for information, to ask how things have happened, where things have gone wrong, to request access to data to actually establish what happened and these reports should offer quite a lot of information for parliament to work with. Parliament in Germany, as I mentioned earlier, goes beyond its usual remit on one occasion when there is a threat to the nation as a whole, national security threats of the highest order. That is where parliament, in the form of a special commission, itself authorises surveillance and only parliamentarians can say to go ahead or not to go ahead. That led to a constitutional court case some years back because individuals felt this denies them access to the courts. That is a problem in terms of the balance of power between the institutions. The court came down five to three in favour of this existing model with substantial criticism, of course, because access to courts and the role of the judges is extremely important and should not be curtailed lightly. Data protection is a joint effort and it is not just parliament but the courts themselves which should play a strong role. I think the judge, if there is enough manpower for that, is a good person to actually authorise specifically important or infringing measures. There are the independent bodies and the commissioners. Again I would like to stress the importance of internal measures within public authorities. That is very important and more can be done there I think.

Q761 ***Lord Norton of Louth:*** It is almost a passive role for parliament in terms of being the recipient. Is there more it should be doing?
Professor Oliver: I do think it is important to distinguish, at the moment at least, between the House of Commons and the House of Lords because your chamber is much more independent and there is not a government majority, and for all the reasons that we know one can rely on the House of Lords to make it much more difficult for the government to legislate in ways that give too much power in relation to surveillance and so on. Whether that would remain the case as and when the House of Lords becomes largely elected is a matter we cannot go into. When it comes to parliamentary procedures, I myself am very

interested in the idea that committees scrutinising Bills and Draft Bills could develop standards against which Bills, or provisions in Bills, that are to do with surveillance would be tested. My own sense is that those standards could partly be developed by committees themselves so after a period when several Bills have been looked at you will find a committee is repeatedly getting concerned about whatever it is and you could say that is the standard. My own sense is that does not prevent parliament voting for this thing that seems to be contrary to standards but at least it is not going to be done by mistake. It should feed back into the governmental process where Bills are being drafted because then the minister will be able to say "we are going to get in trouble with the House of Commons, or whoever, if we do it. We want to do it but let us brace ourselves". I think that would be entirely desirable.

Q762 ***Lord Norton of Louth:*** From your previous work I believe you ascribe quite a role to this particular Committee.
Professor Oliver: Absolutely, yes.

Q763 ***Lord Rowlands:*** Your reply promoted the question I was about to ask. We have seen a lot of evidence about privacy impact assessments within government departments. Would it be a good idea that any department bringing a Bill before the House would have to undertake a privacy impact assessment and publish it and reveal the degree to which it has assessed what impact this Bill will have on privacy matters?
Professor Oliver: That sounds like an excellent idea.

Q764 ***Lord Rowlands:*** We can build powers into the legislative process. Do you think that individual privacy is sufficiently protected by the common law in the United Kingdom?
Professor Oliver: No, I do not. It has made enormous strides, partly under the influence of the Human Rights Act, in relation to privacy and the press. I think individuals do now have a great deal more protection against the press than they did some years ago but it does not say much about relations between the individual and the state or other relationships which are not to do with the press. There is a lot to be said for common law development: it is incremental, it is trial and error and it avoids the political disputes you get. If the government were to introduce a Bill about privacy you would get Fleet Street up in arms and then it is difficult but if the courts do it they get there. But I think there is a limit to what the common law can do.

Q765 ***Lord Lyell of Markyate:*** This question follows immediately on from that. To what extent are issues about privacy likely to be resolved by the courts in the future? We have the recent Murray case, the J K Rowling case. We had the earlier case of Mr Justice Jack where the Court of Appeal thought he had gone a bit too far in limiting the powers of the press. Some of us in this Committee are worried that judges will be limiting freedom of speech, which is another very important aspect even though it is sometimes unpleasant. To what extent do you think the courts are going to get this right and provide the right balance under the Human Rights Act?
Professor Oliver: One can only guess. I do have quite a lot of faith in the ability of the courts to find balances. There are conflicts between the freedom of the press and privacy, and where you draw the line is not easy, but it would not be any easier if the idea was that there should be an Act setting it out. One can imagine the Act would go on and on about things. The Human Rights Act already has this peculiar provision about the importance of freedom of the press in it and I think a statute about it would have many, many more of those. I just happen to like judges and I like the common law method and I have a bit of faith in it but I do not believe it can solve all the problems.

Q766 ***Lord Morris of Aberavon:*** I am concerned about the Data Protection Act and how far it is an adequate organ for the privacy of citizens' personal data to be protected. The exceptions and exemptions created under the Act, are they too broad and should they be narrowed? Is not the Act itself contradicted by the Freedom of Information Act?
Professor Fedtke: A Data Protection Act is an enormous advantage in whatever form because it does provide a very thorough broad basis on which public authorities and citizens can draw in the absence of specific legislation. Specific legislation is more helpful, as I said again and again, to actually identify specific dangers and balance them to the aims of public authorities. As far as the exemptions are concerned, it is true that the Act does specify a long list of exemptions and that begs the question what happens if these exemptions are invoked, what regime will take hold in the absence of the application of the Data Protection Act. The answer again is design specific legislation for those particular areas, whether it is media which have exemptions under the Data Protection Act, whether it is security agencies which have exemptions under the Data Protection Act or whether it is the police which have exemptions under the Data Protection Act. I would try to design special statutes which address those specific areas. In that case, I do not really see a problem with the fact that the Data Protection Act is not applicable across the board because that will not be the case in a system like Germany because special legislation will kick in. How do you define particular aspects? How do you define national security, for instance, which is one of

the grounds for an exemption? It is very difficult to phrase that in detailed terms. The Data Protection Act, as it is, is a very substantial piece of legislation already. If you try to introduce additional interpretations to make that more specific and to make the exemptions more workable, that could double the size of the Act at the end of the day. That is one of the main problems, the definition of these exemptions, to try to find language which specifically says under what conditions there will be an exemption. That is the main problem and that is where the data protection is quite broad at times and leaves a lot of flexibility and room for interpretation.

Q767 ***Baroness Quin:*** Professor Oliver, at the beginning you talked about your concerns about sharing of personal data between departments of government but I wanted to ask about the sharing of personal data between the public and the private sectors and how concerned you are about that. Does that undermine any constitutional safeguards or principles and is the private sector in some way less constrained than the public sector?
Professor Oliver: There is a concern. There was an example in the news a few days ago where the social security department was talking about sharing information with the power supply companies about which people were on benefits so it could check that people were on the right tariff, so poor people got the low tariff. I was rather horrified at the idea that, without thinking about the implications of disclosing information to private bodies, particularly about somebody's poverty or their income level or whatever it was, the sharing of information should be suggested without evidently the minister in question thinking it was a peculiar thing to do. I am a bit concerned about the sharing of information with private bodies and that is just an example. The government possesses pretty personal information which we hope they will not abuse, but private power companies or Tesco might well. It worries me, and it worries me partly that there does not seem to be a culture in government that sets alarm bells ringing and asks "is this something we should do?" Maybe there should be a code somewhere or statutory provisions to limit that.

Q768 ***Viscount Bledisloe:*** I have a related question about retention of data. We were told that if the police ask somebody who is on the scene of a crime but is not a suspect for his DNA or his blood because they want to eliminate him, unless he actually says at the time "I want that torn up after you have finished this investigation" it will be kept forever, or virtually forever, and can be used for other purposes. Do you think that is the right way around or do you think he should be asked at the end of the inquiry shall we destroy it or can we keep it?
Professor Oliver: My own sense is there should be a presumption that it should be destroyed unless the person in question specifically agrees otherwise.
Professor Fedtke: I would go one step further and say not just a presumption that it is destroyed but a clear timetable when data has to be destroyed, again specific data and specific instances. DNA is extremely important, sensitive information. I think there should be a clear rule saying after one month, after three months, after the close of the investigation. There should be a clear time line rather than just a presumption a public authority will do it. There should be statutory provision which says so.

Q769 ***Viscount Bledisloe:*** It may well be that the inquiry is rolling on forever. I would have thought they could keep it as long as the inquiry was alive rather than for a set period of time. Would that not be better?
Professor Fedtke: Absolutely. It depends on the context. Data is extremely contextual and its importance in the way you deal with it is relevant. Of course if you have a criminal investigation which drags on for a long period of time you would not want data to be destroyed within a month or three months. Of course you wait for the formal close of that investigation and then say from that point in time we will ensure that data is destroyed. Another brief idea here when it comes to the erasure of data, I would look closely at internal safeguards. Public authorities should be under a duty to document that data was destroyed or erased from data bases on a particular day, at a particular time, by a particular officer so there is a paper trail of what public authorities do with the data they have retained and are supposed to destroy. You could add that that particular function, destruction or erasure of information, is to be placed under the scrutiny of one particular high-ranking official possibly with a special legal qualification. You can introduce different levels of control within the public authority to ensure that destruction of data is done.
Chairman: Can I thank you both for being with us and for the evidence you have given which is greatly appreciated.

WEDNESDAY 11 JUNE 2008

Present	Goodlad, L (Chairman)	Peston, L
	Lyell of Markyate, L	Quin, B
	Morris of Aberavon, L	Rodgers of Quarry Bank, L
	Norton of Louth, L	Rowlands, L
	O'Cathain, B	Woolf, L

Examination of Witnesses

Witnesses: Councillor Hazel Harding CBE, Ms Donna Sidwell and Mr David Holland, Local Government Association, examined.

Q770 ***Chairman:*** Councillor Harding, Ms Sidwell and Mr Holland, may I welcome you warmly to this committee and thank you for coming? We are not being televised but we are being recorded. Could I ask you to identify yourselves for the record?
Ms Sidwell: My name is Donna Sidwell. I work for LACORS (Local Authority Coordinators of Regulatory Services). We are here on behalf of local authorities in England, Wales, Scotland and Northern Ireland and the Local Government Association, Welsh Local Government Association, Convention of Scottish Local Authorities and Northern Ireland Local Government Association.
Councillor Harding: I am Hazel Harding and I am Leader of Lancashire County Council and I am the Chair of the Local Government Association Safer Communities Board.
Mr Holland: My name is David Holland. I work for Cardiff Council and I have the consumer protection brief for that local authority.

Q771 ***Chairman:*** Thank you. Could I begin by asking about closed-circuit television? Do you think that the apparent ineffectiveness of CCTV that we read about in the newspapers in preventing antisocial behaviour and crime in public places justifies its continual proliferation throughout the country and by local authorities?
Councillor Harding: My perception and that of my colleagues from various councils is that CCTV is very popular with law-abiding members of the public who see it as a preventative and feel much safer. Because crime levels and some forms of antisocial behaviour have fallen, what we are dealing with now in many very safe areas is a perception that people have that they are not as safe as they used to be. CCTV is something that councils are facing demands for day after day from members of the public who think it would actually make them safe and they would feel safer because of it. There are some good examples of how CCTV has helped perhaps not always to prevent but certainly to detect crime and as such it has been very useful. A very good case in point is Ipswich where the dreadful murders of the women working on the streets were solved quicker because of the CCTV coverage. Actually it was Ipswich Council's CCTV which placed the girls in particular places at certain times and also the eventual killer who was caught. The police accepted that it was faster because they were able to see where the victims and the perpetrator were. It was a very good example of how in fact crime was probably prevented because I do not think, short of being caught, it was going to stop at that point. That is an extreme example and a very tragic one. In terms of antisocial behaviour, I do not think necessarily that people out on the streets sometimes causing mayhem look at where the cameras are or behave differently because of it, but I do think that it does enable prosecutions and, as such, is very useful. Many of the CCTVs, though, that actually record antisocial behaviour are not council-owned; they are owned by local businesses. Most of the council ones are actually monitoring traffic.

Q772 ***Baroness Quin:*** Probably all of us have seen very fuzzy pictures from CCTV. Is your impression that the technology is improving and it is becoming more effective? Obviously they have been around for quite a long time now.
Councillor Harding: Yes, the quality of the cameras does make a huge difference. Digital images are much more easily seen and people are more easily identified if there is better quality, and they are improving.

Q773 ***Lord Rowlands:*** Could you help us to explain what procedures and processes a local authority goes through before it establishes these cameras? For example, in a high street or a park, what process does the local authority go through by way of consultation and assessment of privacy issues before establishing the cameras?
Mr Holland: I will try to answer that. My answer would be based on my experience in Cardiff. Our CCTV codes of practice are designed against national guidance and they are designed in consultation with the police, with our own legal service and I guess we are very much looking at the

core function of a local authority, which is to protect and serve the local community. Yes, we want to bear in mind people's right to privacy. For me, the overriding role for the council is to protect its community. The rotation of those cameras is primarily, as Councillor Harding said, about traffic flows in a city like Cardiff. If the cameras are located in parks and high streets and other areas that have attracted complaints of nuisance, for example on an International day in Cardiff when the streets are very full and they stay very full in the evenings as well, they are located at the request of the police to make sure that law and order is observed and that people can come into Cardiff, enjoy the day and go away and want to come back again. I think that is very much what the council wants to achieve.

Q774 ***Lord Rowlands:*** Is there a form of planning process? What sort of process takes place?
Mr Holland: Every time the CCTV code of practice is reviewed, consultation will be carried out internally and externally with community safety partnerships and the like to establish the scope of that code, what it should cover and how those cameras would be deployed. That is set out in Cardiff's code. I would suggest if every council has a similar code those can be produced to a committee in evidence, should it wish to see them, so that you can see the issues that are considered about the location of CCTV.

Q775 ***Lord Rowlands:*** How do you assess privacy issues in that context?
Mr Holland: The privacy issues will look into things like the Regulation of Investigatory Powers Act, which perhaps we can talk about afterwards, and around whether it is necessary to have those things in there and whether they are a proportionate response to the issues under examination.

Q776 ***Lord Morris of Aberavon:*** What is the interface between local government and the police on these issues? When I was an MP I spent a pleasant quarter of an hour in the Chief Constable's office in Carmarthen looking at what had happened on the previous Saturday night in Carmarthen: antisocial behaviour, actions of ruffians and violence. I do not know why it was in the police headquarters' office. What is the interface?
Mr Holland: The interface is regular. Local authorities and police officers now spend a significant amount of time together. Under partnerships that are formed under the Crime and Disorder Act, we both have a statutory duty to reduce crime and reduce the fear of crime, which is something Councillor Harding was alluding to earlier. It is a regular thing. My trading standard's officers spend at least two full-time equivalent days a week working with police officers on issues of concern to the community.

Q777 ***Lord Morris of Aberavon:*** That is a matter for local determination. There is no national standard, is there?
Mr Holland: There is the Information Commissioner's Code of Practice on CCTV and a national CCTV strategy. I guess the demand for interaction would depend on the local authority in question. Local authorities are very diverse in their coverage.

Q778 ***Lord Morris of Aberavon:*** Whose pictures are they? Are they yours or the police's?
Mr Holland: At Cardiff the system is owned by the local authority and we have a partnership arrangement with the police. The local authority role is primarily to monitor traffic flows. It is the police that use their part of the system to combat crime and disorder.

Q779 ***Lord Norton of Louth:*** This really follows up on Lord Rowlands' question. In establishing where there is CCTV coverage, you have various criteria that have to be met before you set them up. Once they are set up, is there subsequently a review to determine whether they have met the criteria or are they just left? Are there circumstances where you decide that there is no longer a case for having coverage and actually removing them?
Mr Holland: Cardiff's CCTV code is periodically reviewed by a number of people like the stakeholders themselves and the Community Safety Partnership. It is looked at by the Office of Surveillance Commissioners when they come to do their inspections under RIPA, if I may use that acronym. It is examined on a number of different occasions and, yes, we are always asking ourselves: do we need to do it, is it necessary and is it proportionate? Those are the questions that the OSC will ask us and we want to be able to be in a position to answer that and say, "Yes, it is, because we still have issues in our community that we need to resolve".

Q780 ***Lord Norton of Louth:*** It is not that any have been withdrawn; it is just a case of more and more CCTV cameras being put up?
Mr Holland: I am not aware of any having been withdrawn. I am aware that the Government is providing local authorities considerable amounts of money for CCTVs.

Q781 ***Lord Lyell of Markyate:*** I think you are discussing overt CCTV cameras which the public can see are there. One of the points is that they will see it and either be deterred from misbehaviour or comforted that the matter is being watched. We shall no doubt be asking you a lot of questions about the difference between overt and covert, but what you are answering is overly overt, is it not?

Mr Holland: I think I am talking about mass overt surveillance, yes.

Q782 ***Baroness O'Cathain:*** What sort of reliability do these CCTV cameras have? One gets the impression that sometimes they are not working properly. Following on from that, what sort of drain on local authority finances is there in the maintenance of these cameras?
Mr Holland: I can only answer for my own local authority. They are fairly robust. We still use VHF videotapes in this day and age and we use those 12 times and then they are discarded. As I say, the Government is providing significant amounts of money to maintain CCTV and the main drive is around the reduction and detection of crime and disorder.

Q783 ***Chairman:*** Before I come to Lord Peston, can I just ask what the Local Government Association's Safer Communities Board actually does to ensure that CCTV is used in a manner consistent with civil liberties and human rights and whether the guidance from the Information Commissioner's Office and the Association of Chief Police Officers and other national agencies is of any relevance to what the LGA's board does?
Councillor Harding: Certainly the LGA participated in the implementation of the National CCTV Strategy alongside the Information Commissioner. We would always advise councils of the need to ensure that people's civil liberties and human rights were taken account of.

Q784 ***Lord Peston:*** When I used to take an interest in local government finance, it was to do with local government providing a variety of services, notably education. For reasons which I neither understand nor approve of, this Government seems to have turned against local authorities in the field of education. It would not have occurred to me—and I am talking some time in the past—that the provision of safety and security was a local authority function. Has it become a local authority function because you cannot find other things to do with yourselves?
Councillor Harding: Not at all, and certainly if I look at my own authority, and I think you would find it reflected across the piece. We regularly ask residents what are the most important issues for them. The number one issue for people in Lancashire, and we have more than one million people living in Lancashire, is to feel safe. I think it is more than something people aspire to; I think it is a basic human need. You cannot do all the other things they tell us that they want to do unless you feel safe, and that is safe in your home and safe on the streets. The police would acknowledge that they cannot help people to feel safe on their own; it is a matter for local authorities and for other partners as well.

Q785 ***Lord Peston:*** You yourself did raise what you might call the distinction—and this committee has been bombarded with this distinction—between the public perception of feeling safe and the reality. I live in Suffolk, not far from Ipswich for that matter, and I would guess if you read the local papers in that part of the world that the public perception is that it is not a very safe place. The reality is it is an indescribably safe place. What worries me a bit is that no-one seems to be speaking out by saying, "What is the fuss all about?" It is rather like the ghastly thing in today's newspapers that we are going to run out of petrol. We are not going to run out of petrol but nonetheless to sell newspapers that is the headline the press puts in. Do you have a role yourself, apart from putting the cameras up, of trying to get over, and it depends where you are talking about, that this is a very safe part of the country rather than the reverse?
Councillor Harding: We do indeed and I think that is something we spend a lot of time and effort doing, both in person and through our council publications and through as many means as we can, because it horrifies me when I meet elderly residents who tell me, "I lock my door at 4 o'clock and I never go out". That is not quality of life; that is self-imprisonment, and that is in a very safe part of our county.

Q786 ***Lord Peston:*** My last supplementary is this. You used again the expression "safe in your home". As we have taken evidence, certainly one of my worries is that I do not feel safe in my home but what is threatening me is not thugs but perfectly reputable bodies using the latest technology who look as if they can pry into my home and find out what I am doing. The more I hear the evidence, no-one is protecting me at all. We have referred to those cameras but we have heard of these parabolic microphones you can now use so you can hear everything one is saying in one's home. Do you have any concerns about what is happening with the technology?
Councillor Harding: I think the technology is there if people want it. It is certainly not used by councils to do that. Quite honestly, if someone were directing that at my home, I think they would be bored in a very short space of time. They would not find anything of interest or use to them.

Q787 ***Lord Rowlands:*** We have been on this inquiry for some time now and we have had witnesses. One major witness said that every CCTV system should be approved by the Information Commissioner rather than it just being a local decision. I would be interested in how you would view that, presumably adversely. Secondly, we have received really quite a lot of information from both the police and from all

these reports saying that people may want cameras to be safe but in fact they are of very marginal value in safety. How would you answer those two issues?
Councillor Harding: I think I would probably agree with that last point. Certainly my experience is that there was a proliferation of cameras and demands for cameras. I think the demand is still there but I think that if you were to talk to local authorities and their partners in the crime and disorder partnerships, they would feel that they have addressed what they felt were the most necessary areas, the hotspots in fact, and are resisting calls from residents for any further cameras. With the exception of one or two town centres, I think the police and local authorities would say that they do not necessarily want more systems.

Q788 ***Lord Rowlands:*** What about the role of the Information Commissioner in determining whether new systems should be established?
Councillor Harding: I am always going to say it should be local determination; it should be the people who know the patch, who know the issues, who make those sorts of decisions.

Q789 ***Lord Morris of Aberavon:*** I want to ask you about the abuse of the Regulation of Investigatory Powers Act. I read in this morning's *Times* that Lord Stevens, a former Commissioner of Police for the metropolitan area, says that the security case for extended detention had been undermined by the outrageous abuse of surveillance powers to spy on litter louts, benefit cheats and petty offenders. For local councils to be using such powers brings the whole security issue into disrepute. What do you say about that?
Mr Holland: I have brought my own press cuttings and they are in a similar vein. This one is about phone spies. These are both in the *Mail*. The headline is: "Town halls using anti-terror powers to bug residents' calls"; "Fact File: what the law allows. RIPA gives all councils the right to use overt techniques to spy. The powers are enjoyed by 43 police forces" et cetera; "Council bugs phone call". They are lovely headlines but totally incorrect. There has been a large amount of inaccurate press coverage and we are very grateful for the opportunity perhaps to clarify to this committee what a council can do. Let me be clear, first of all, that a council cannot intercept text messages; it cannot listen to phone calls; it cannot pop round tomorrow and bug your telephone. The Council cannot do that. The Council can undertake what we call directed surveillance, but our powers are quite limited in what we can do. Police forces and security agencies have a full range of RIPA powers; local authorities do not. I think we have said that our role as a council is to protect and serve the local community. I will be frank with you; I will use every power I have available to do that because there are some real rogues out there that prey on the vulnerable and elderly. In working with the police on things like distraction burglaries and the like, the typical victims are single females around 79 or 80 years of age. What we have seen in Cardiff and in many other cities is that these people have lost thousands of pounds to rogue traders, to conmen. That is totally unacceptable in my book. I will use whatever powers I have available to bring those people to book, but I will work within the law. I will work within RIPA and I will make sure that if my officers choose to undertake or apply for directed surveillance that that application is an absolutely necessary use of that power and that it is a proportionate response. I think I can say that for all my colleagues across councils. The press coverage talks about councils using these covert surveillance techniques to watch youngsters buying alcohol. You only have to go out on your streets in your communities to see some of the havoc these young people are causing in communities because of alcohol and wider social problems. Councillors like Councillor Harding and members of neighbourhood watch groups demand that the council do something about it. We use directed surveillance techniques sometimes to do that.

Q790 ***Lord Morris of Aberavon:*** I am sure from your evidence that that is an accurate picture regarding the City of Cardiff, but it seems that there is allegation after allegation and Lord Stevens is a particularly impressive complainant whom we cannot ignore. Some of the allegations are that RIPA powers intended to tackle terrorism and other serious crime—and that was the intention—are used for such things as finding out whether families are in a particular school catchment area. Have you any idea of that and can you comment on it?
Mr Holland: Dare I suggest that the Regulation of Investigatory Powers Act was created to regulate the use of surveillance by public authorities; it was not entirely created for anti-terror powers. The human rights legislation came in with the 1998 Act and RIPA was put on the statute book to make local authorities accountable for what they do when they choose to take actions that would breach Article 8 rights. So it was not just about anti-terror. I think it is incorrect to say that; it regulated the actions of a wider range of public authorities in the way they undertake their regulatory duties. I think you are alluding to the Poole council case where their education services undertook directed surveillance, which has been in the press again. I have spoken to the officer who made that authorisation for the directed surveillance to be conducted. He did so. He went through the RIPA regime; he went through the necessity tests; he went through the proportionality tests and determined that it was an appropriate use of those powers. I hear

lots of people say that that should be judged by magistrates or the judiciary, but every day we see decisions in the magistrates' courts that are amended in the upper courts. The gentleman in question went through a regime. It is all documented and he is accountable for what he did and the decisions he made. Previous to RIPA coming on the statute books, that did not exist. I think that there is an effective safeguard in these issues but we can look at why those processes took place. I need to point out to you that in the Poole incident, while the press have homed in on the fact that a family was spied upon, they were entitled to send their child to the school. There were two other directed surveillance authorisations undertaken which showed that those two children did not live in the catchment area and the places were refused. In the three cases in which Poole undertook surveillance, two of them were justified and two places were refused for a school which people are clamouring to get into. I listened to an interview on the radio with local people ringing in and they said, "Damn right, the council should make sure that only people who are eligible for the school are able to do so". It attracted a lot of public support.

Q791 ***Lord Morris of Aberavon:*** You would favour the use of the Act for all these issues without turning a hair?
Mr Holland: No, I do not think I said that. I am an authorising officer in Cardiff. My role is to protect people's human rights; it is not to rubber-stamp my officers' wishes to go out and watch somebody. I am quite clear about that. It is my job to protect the rights of my community against those unlawful intrusions. I go back to whether it is necessary for us to do it. Do we have to do it? Why do we want to do it and what are we going to do with the product of those things? I am absolutely clear on that. I can tell you that this year in Cardiff I have authorised six applications, and that is all, for directed surveillance; four of those are for what we call loan sharks, illegal money lenders, who really are causing significant difficulties in the south Wales valleys. That may give you some indication of how seriously I treat these points.

Q792 ***Lord Lyell of Markyate:*** Mr Holland, I think you recognise that really your justification is that wicked things happen. After 40 years at the Bar, rogue builders, people preying on elderly people, yes, these are wicked things. You are therefore saying that you think it right that we should live in a society in which local authorities have the power covertly, secretly, to survey us all whenever they think it right, so long as they can show that they are trying to stop something that is wicked. One can understand that argument.
Mr Holland: I am sorry if I gave you that impression. That is not what I said.

Q793 ***Lord Lyell of Markyate:*** You did, very strongly. There is an argument for it but it has to be balanced over whether we want to live in a society in which public officials decide that they will snoop on anybody who they think may be doing something wrong so long as they have some reasonable case for thinking they may do it wrong. Is there not a balance? Ought not Parliament to say that some of these covert activities should be reserved for very serious offences indeed and terrorism, whereas other things which are wrong—cheating over school catchment areas if that is happening and so on or dog fouling—are certainly not sufficiently serious for covert activity. Certainly with dog fouling it should be overt; you should know that there are cameras in the park. It is a worry to this committee, it is certainly a worry to me, that you have justified to yourself over-strong powers.
Mr Holland: Let me see if I can redress that. Most of a local authority's duties are placed upon it by regulation and most of what we do in administering that legislation is done overtly. I think I said to you that I authorised six in 2008. I should have told you that on illegal money lending I have a remit to operate a unit that covers the whole of Wales. It is not just six in Cardiff; that is six across the whole of Wales. If we can do something overtly, then clearly we will. I do not think we need immediately to make recourse to RIPA and say, "Here is the chance to go snooping again. Terrific! What shall we do today?" That just does not happen.

Q794 ***Lord Lyell of Markyate:*** That is not the point I put to you. The point is: are there not degrees of seriousness which have to be considered when you decide what surveillance powers should and should not be allowed?
Ms Sidwell: Perhaps I could add to Mr Holland's debate. There are certainly different degrees of seriousness. You are quite right in what you were saying. There will be those occasions where it is more appropriate for covert surveillance to be used, for a covert human intelligence source to be authorised or for subscriber or billing information to be obtained. We would argue that the checks and balances already in place are fairly good at enabling a local authority to assess on necessity and proportionality grounds. There are some occasions when you may challenge the decisions that have been taken and you might say that if you were looking at it from the judicial perspective a different decision might have been taken. I think there are areas where additional guidance can assist and working with the Home Office, the Office of Surveillance Commissions and the Office of the Interception Commissioner can help

us in that. We participate in an ACPO peer review group in all of those areas where the legislation can be clarified. Mr Holland quoted the case of C v the Police and Secretary of State for the Home Department [14.11.06] IPT/03/32/H before the Interception Tribunal in which Lord Justice Mummery states: "The experience of the tribunal over the last five years has been that RIPA is a complex and difficult piece of legislation." I think that is very true. There is a further debate to be had, and the exercise you are undertaking at the moment will be very valuable in this in helping the non-enforcement community of local authorities to get more clarity on some of the issues on when authorisations should be given. I see that the work we are doing with the LGA, COSLA, NILGA and WLGA can help in that process. We want the local authority communities and residents to be confident and to believe that they are not being snooped on. We strongly do not believe that is the case.

Mr Holland: If you look back at Hansard you will see that local authorities pushed hard to be included in the RIPA regime because we want to be accountable for what we do. If you take us outside the RIPA regime, that does not automatically preclude us from carrying out our regulatory duties.

Q795 ***Lord Lyell of Markyate:*** But it may limit the way you do it and that is really what we are talking about.

Councillor Harding: I am a lay person in terms of RIPA but I am very much aware that some of the people that we are dealing with in trying to enforce the law are becoming cleverer at the way in which they break the law and avoid detection. They use all sorts of technology in order to avoid being detected. I think that I am reassured by the fact that RIPA is not being used in a wrong way; it is being adhered to by local authorities. Equally, we are not talking about somebody dumping an odd bag of rubbish when we talk about fly tipping; we are talking about massive dumping of tyres and of builders' waste time and time and time again. If we need to look at somebody's telephone records in order to ensure that we catch a perpetrator, then I think it is something we need to do, but it is not undertaken lightly or in any way to catch the person leaving the odd bag of rubbish, though that is equally reprehensible. It is about the large-scale, frequent offenders in many of these cases.

Q796 ***Baroness Quin:*** In terms of the retention of the data that you get, in the six cases that you mentioned how long would the data be kept for and who would have the responsibility for deleting or removing that data?

Mr Holland: Any product of a surveillance exercise, any papers relating to the application, would be held in accordance with the codes of practice that have been issued. They would be held in accordance with our data protection protocols. They would be made available to the Surveillance Commissioners, should they request to see them, or in a court of law, should there be a request to see those in any subsequent proceedings. They are kept under lock and key and the people with access to that have a full and clear understanding that they are personally responsible for the security of that data.

Q797 ***Baroness Quin:*** Is there a time limit on that?

Mr Holland: The codes talk about referring back to the Criminal Procedure and Investigations Act. If there is no likelihood of that material being used in another case, then it will be destroyed and deleted.

Ms Sidwell: Generally the maximum they would be kept is six years.

Q798 ***Lord Peston:*** Going back to Lord Lyell's point, his point, if I may interpret him, is about proportionality. It seemed to me you demonstrated beyond a shadow of doubt that he was right and in some sense you are wrong because when you are talking about money lenders or large-scale dumping and those kinds of examples, I think none of us would doubt that that is the kind of area where we want you to see these drastic powers used. But in the end this is a school catchment area. It is rather like deciding that the local church school is the best and suddenly you announce, never having been near a church for 25 years, that now you are devoted to the deity and all that. In the end, most rational people shrug. If there are a few people around lying, you do not want it to happen, but you would not use your major powers compared with the fact that it is partly a matter of allocating resources. I am with you all the way: every time you catch a money lender or a major persistent dumper, I say more power to your elbow, but as for catching the odd person fiddling the school catchment area, my response is "so what?" It seems to me Lord Lyell has elicited from you the need for a balanced response, and that is really all we are trying to get to in our approach to this subject.

Councillor Harding: May I say that I would agree entirely but I think if we are talking about proportionality, you would find that the Poole case was a very rare occurrence. Certainly my local authority has never used it for school catchment areas and I cannot foresee a time when we would. It would be wrong, I think, to prevent local authorities using it in the way in which the vast majority of local authorities do for those extremely serious cases on the back of one authority deciding to use it for school catchment areas.

Ms Sidwell: You mentioned that surely local authorities would agree about not allowing dog fouling in this vicinity. Generally, that is what is done. It is rare for surveillance to be used in this way. Other areas where I know there have been debates with the Surveillance Commissioner are where you get instances of noise nuisance; mostly local authorities will actually write to the resident and say, "We have had complaints about the noise emanating from your residence. Please can you desist? If you fail to do so within this timescale, we will undertake some surveillance". It is overt; it is not covert. If it is anything you could hear if you were walking down the street, in our view that is not something that would be a covert matter because it is something any member of the public could hear.

Q799 ***Lord Rowlands:*** For clarification, Mr Holland you kept on using the words "direct surveillance". Is there any difference between direct surveillance and covert surveillance?
Mr Holland: Covert surveillance can perhaps be split into what is directed surveillance, watching the movements of people and intrusive surveillance is something restricted to the police and the security agencies, which involves bugging people inside their homes, et cetera, something that would happen on a private vehicle or in private premises.

Q800 ***Lord Rowlands:*** Directed surveillance is a part of covert surveillance?
Mr Holland: Yes.

Q801 ***Lord Woolf:*** In what you have been saying you have identified that there are various different categories of surveillance. I think what has been causing concern to the committee is your general approach seemed to be: we have the powers; the public would like us to use the powers; they can be beneficial in detecting things, and so we use the powers. That may not be a fair picture. What I would like to find out is: to what extent, in coming to your decisions, do you have in mind all the time how much importance you attach to the fact that if you were to ask the public if they want unnecessary surveillance, they would seek equally to say they would not want unnecessary surveillance and surveillance in itself can be a bad thing just because it happens.
Mr Holland: I would agree with you. I am sorry if I have not said it enough times. My considerations and those of my colleagues are: is this covert surveillance necessary? That is the first test. If it is not necessary, if we can achieve what we want to achieve—the protection of the community—by other means, then we do not need to undertake covert surveillance at all. The first test is on necessity. If there is a necessity to do it, if we cannot protect the community by normal routine means, then we consider is it a proportionate response? I think we go back to the Poole case. The authorising officer in that case was provided information. His education officers had said that they had tried their normal means to determine whether these children are eligible or not; they still had a doubt. He applied the test of necessity, proportionality, and determined in his mind that surveillance was appropriate. That is what authorising officers are challenged to do. Is it necessary? If it is not, we stop. We do not undertake unnecessary surveillance. Even if it is necessary, is it a proportionate response? If it is not, we do not do it. I am sorry if I have given you the impression that I charge off and snoop on everybody at every chance I get because that is not the case.

Q802 ***Lord Morris of Aberavon:*** Where do you draw the line?
Mr Holland: It is almost a quasi judicial role, is it not? I am presented with a body of evidence by my officers and I have to apply not only the Act, the codes of practice, but the guidance from the Office of the Surveillance Commissioner, and at times I have rung the local OSC inspector and asked his observations: What do you think? We have guidance through LACORS. We are trying to find our way through a complex, difficult piece of legislation. If you read the OSC report, you will see that even the law enforcement agencies, the police, are having their own difficulties in finding their way through RIPA because there is a dearth of certainty on the law. There is very little in the courts that has given us guidance. If you want to ask me about the Trade Descriptions Act, I have 40 years' worth of guidance there but perhaps some of you have sat in judgment on section 1 of the Trade Descriptions Act and have discerned what it actually meant, what Parliament's intention was. There is very little on RIPA. I try my best. I look at guidance. I seek guidance from the inspectorate and from colleagues, but the decision on whether it is necessary and proportionate sits with me as an authorising officer as it would with a superintendent in the police force.

Q803 ***Lord Rodgers of Quarry Bank:*** I think it follows from these sensitive and difficult issues that I want to turn to the views of the Chief Surveillance Commissioner. I am referring to the annual report for 2006-2007, chapter 10, which is Inspections of Local Authorities. I have to say I find this very disturbing. May I quote one or two cases? In paragraph 10.2 the Commissioner says: "I have been disappointed with the local authorities that have failed to act on the recommendations of previous inspections." Then in paragraph 10.3 he says: "There has been improvement but it seems that some authorities did not expect the more in-depth inspections conducted this year." It goes on, "well

meaning but inadequately informed." I think this is extremely depressing but I hope you will give a justification. You may have an explanation for why these things should go wrong and what can be done to do it better.

Mr Holland: I too have the report in front of me. In 10.2 he also says that "the general standard of compliance with the statutory provisions continues to improve. He also says that the number of faults reported last year has reduced." We are moving forward but we are not getting it right every time. If you go back into section 8 of his report, which is the inspection of the law enforcement agencies, he makes similar comments. In fact, he had to order some re-inspections of two law enforcement agencies in 2007. He makes similar comments about government departments. I think the challenge for local authorities is that there are 474 councils and that is a significant challenge, given the different localities that they are required to govern at district, unitary and county level. It is a big challenge for the Local Government Association to move us forward, but I think we are getting there. Do you mind if I go to the Interception of Communications Commissioner's report for 2006 for communications data?

Q804 ***Lord Rodgers of Quarry Bank:*** I know it is getting better. I accept that entirely, but how far are you going to get it to 99 or 100 per cent? Could I ask the question, if I may, to Councillor Hazel Harding to find out what her views are on the matter as an elected member of the authority?

Councillor Harding: I am always disappointed when there are reports that say "could do better" for local authorities. I am not surprised because you are only ever as good as the individual authority or the individual within that authority. I am very proud of my council; it is a four star council, but I keep saying to people who work for us, "excellent does not mean perfect", and it does not. It would be very strange if we did get to a point where we were claiming perfection. I think getting better but not fast enough would be my reading of the report. I would hope that from the LGA we can support councils that are seen not to have made those improvements in getting better.

Mr Holland: I think it is easy to criticise local authorities and our efforts to be RIPA compliant. As I have shown you earlier, you can make a good story out of a totally inaccurate statement. We are moving forward. Last year the local authorities pulled together a number of road shows with ACPO, NPIA and the Home Office—and that was at our instigation—to go across the country to pull together practitioners to talk about these challenges posed by RIPA. We keep going back to this statement by Lord Justice Mummery that this is a complex, difficult piece of legislation. We are seeking to move forward. Ms Sidwell sits on a committee with the Association of Chief Police Officers (ACPO). In my own authority we work with the South Wales Police to make sure our procedures reflect theirs. In Gwent five local authorities work with the Gwent Police Force to do exactly the same thing. We are trying to move forward to get this right, but it is a difficult task.

Ms Sidwell: We know that the Home Office has undertaken a RIPA review over the last 12 months or so. There is a huge amount of work that can be done to assist local authorities and the other enforcement bodies. The codes of practice on surveillance are almost a mirror image of what we have in the legislation. Having more explanatory notes there to assist on issues like privacy and some of the more detailed collateral intrusion issues can really help those that are looking at it from an enforcement perspective, and having consistent training, making sure that the authorising officers are well versed in the human rights principles, as we already believe they are, but having additional training that is of a sufficient standard that you as members of the Lords and local communities are assured of the work that is being done.

Q805 ***Baroness Quin:*** I want to raise the issue of data sharing between agencies, sometimes that seems to be a good thing and for example the lack of data sharing was very much criticised in the Bichard Report following the Soham murders. Certainly, if it is aimed at protecting the vulnerable, one can see very strong arguments for it. At the same time, some evidence seems to be there that expresses concern about data sharing because the information then becomes circulated more widely and there is the danger of people being stigmatised because of something that may have happened which, because of the availability of the data, is rather difficult to live down subsequently. Therefore, I wondered if you felt that the emphasis on sharing personal data does pose threats to individual privacy and the citizen's relations with the state.

Ms Sidwell: If I may start by answering the question, there is an incredibly fine line to walk between respecting the individual's rights to privacy, the protection for the individual, their home and property, and the greater good for the local community. I think that is fundamental in the data protection principles. Every local authority will have policies in place to ensure that they maintain and meet the data protection principles. We have guidance from the Information Commissioner's Office in this area. Data will only ever be retained in accordance with those principles and shared with other agencies through legal gateways that exist. There are many agencies—I can name HMRC—that are incredibly cautious about the sharing of data, and quite rightly so. We respect that and we would treat

personal data in the same way. It should only ever be used if there is a clear legal gateway. An example would be section 35 of the Data Protection Act, which enables the lawful disclosure of information in relation to legal proceedings. So it is a very clear gateway that is clearly defined and requests can be made of other agencies, but they still have to make sure that they maintain and hold the data in accordance with the legislation. That is perhaps partly the discussion. I think from a local authority perspective my colleagues would be able to give practical examples. Perhaps Mr Holland would like to touch on some of the areas where there is data sharing.

Mr Holland: Perhaps I could point you to Sir David Varney's report on Service Transformation: Better Service for Citizens and Businesses. He makes an observation that in the case of a bereavement—and these are his figures—some 44 different public sector agencies have to be informed. One of the recommendations in his report is the development of a service that required the reporting of these facts just once and from there the information is shared across government in a secure manner. That was something that Sir David Varney advocated on data sharing. On issues like registration and bereavement issues—births, deaths and marriages—I think there is a positive sharing of information. His research said that the public is willing to give out that detail if there is a clear benefit to be gained. I think there are some very positive, good examples happening on data sharing inside local authorities. Perhaps that is the best example I can provide at the moment.

Q806 ***Baroness Quin:*** Is there adequate training of people in this area in recognising the fine line that Ms Sidwell referred to?

Ms Sidwell: Most local authorities will have training on data protection issues. I know certainly at my own organisation I did a training session earlier this week for those who were dealing with other people's data on their own databases, on their websites, respecting the individual's personal rights. I would say that as a general policy local authorities will use the guidance we the Information Commissioner provides. Councillor Harding might be able to speak from her authority's perspective.

Councillor Harding: I have some excellent examples of how data sharing can help people and assist them in their daily lives. We tend to do it with people's consent. We have a number of examples where we have had family doctors write to people over the age of 75 with whom they deal on a regular basis saying, "We know you have your health check, but what about a wealth check? Are you getting all the benefits?" We brought £1 million into one district in Lancashire in added benefits to people over the age of 75 who were not claiming things to which they were entitled; it was £2 million in another district. It is of course hugely beneficial to the local economies because those people spend the money locally and the doctors felt the benefit because these people started going to the doctor's less often because they had a little bit more money to spend and felt better. That was a good example, not of sharing the data but asking the doctor to use his data to benefit the people. We do it generally with older people. We will say to them when we have a fire safety check, "Are you sure your home is secure? You have had your fire safety check but would you like your locks checked by somebody reputable that the fire service will recommend to you?" Then if people are also seen to be struggling with other things, we ask "Would you like us to come and assess your needs for social care?" There is an awful lot you can do face to face with somebody where you are asking their permission to share their needs. I think that is very useful and it is a true example of how data can be used to benefit people.

Q807 ***Lord Lyell of Markyate:*** I am sure the whole committee respects local authorities for the very great deal of good work that they do and the effort they put into this. Certainly when you talk about the Data Protection Act, there are a lot of legal fine lines, and I have had to consider them in declaring an interest running a very small business and as a barrister and so on. It is fairly impenetrable. I think what concerns this committee, as Lord Peston was emphasising, is really this whole area of proportionality. Councillor Harding has given very good examples of how beneficial aspects can work. If you are looking, for example, and this is more broad than the Data Protection Act, at fly tipping or illegal money lending, if that is happening in a serious way, then there may be a very good case for directed, covert, whatever you like, surveillance, carefully documented, as it must be, and so on. What is frightening people is this: there was a stupid man in Cumbria who did not quite shut his dustbin, and you will remember that one. This is just a newspaper report: there was some woman, who I thought was a poor woman, who put her dustbins out a day early. They both received quite whopping fines for people like that; it was pretty much their net take-home pay for a week. That is a lot of money for people. People feel that public authority servants sit with a steady wage and a secure job and they are dishing out these large fines. Do you recognise that it is very important to try to educate people and not cane them, if I can use that allusion?

Councillor Harding: From an elected member's point of view, I am appalled when I see some of those examples in the press as well. I hope the elected members in those authorities are equally as appalled because it does seem to me that it is a case, in some

instances, of using a sledge hammer to crack a nut. I also think sometimes the reporting is not always as clear about how many times people have been spoken to, have been asked and advised and that authorities at the end of the road will use the legislation to make their point. I do not think it is always appropriate but in some cases there is a long history of education and support for people before it actually gets to that stage.

Q808 ***Baroness O'Cathain:*** This question refers to the increase in the use or advance in technologies of smart cards, biometric identifiers (and that of course applies to anti-terrorism) and other technologies for controlling personal access to local services, including public transport, libraries, education, leisure and recreation. How do you see that developing and do you think there are going to be many more dangers facing you and the public as a result of this?
Councillor Harding: I always think that Tesco and Asda probably know more about me than my local council does because every time I shop there they have a record of what I have bought; they also have other details which allow them to market things to me. From a local authority point of view, we have schools that are using fingerprint technology for school meals. That is not at our instigation; it is their choice. Children pay their money in and then can access a meal and it comes off their bill. It also means that children who have free school meals can access food and nobody knows that they are in receipt of free school meals. It is a very fair system from that point of view. It was criticised by some parents but the majority of parents thought it was a reasonable idea because they had had a lot of experience of children's dinner money being used in the sweet shop or other places and not to buy a proper meal. This way, they knew their children were getting a decent meal. The techniques are there and are being used. I must say, from my point of view, our library service has opened up its service: you no longer have to take two forms of identification and your birth certificate in order to join the library; you can just join by going in and declaring who you are and saying, "I'd like to join." It seems to me, for a public service, it is a very good way of ensuring that more people use our services than demanding forms of identification. In that way, we are finding out less about people.

Q809 ***Baroness O'Cathain:*** You are emphasising, quite rightly, the positive benefits and all those are admirable. What about the dangers? Do you see any negatives?
Councillor Harding: I think there are. A number of people have referred to being "spied upon" and "being watched" and I do not think any of us like to think that as we go about our daily business we are being spied upon. Knowing how much information is held about us all is a little bit worrying. Certainly you see the bank frauds. I have had my credit card used by other people when it has never been out of my possession. Those are frightening aspects of technology. But the technology is not going to go away, and we have to manage it and we have to ensure that it becomes safer for people to use it.
Chairman: Councillor Harding, Ms Sidwell and Mr Holland, I would like to thank you very much indeed on behalf of the Committee for being with us and for being so generous with your time and for the evidence you have given. Thank you very much indeed.

Memorandum by Dr Eileen Munro, Department of Social Policy, London School of Economics

Introduction

1. This submission focuses on how surveillance and data collection by public and voluntary organisations is changing the balance between citizen and state and, most specifically, how it is changing the balance in the triad of child, parent, and state. Surveillance is being used as a mechanism for screening, identifying and targeting groups of children deemed "at risk" of some adverse future outcome but is being done without an adequate scientific base. Adverse judgments about children and parents will be made in idiosyncratic or opaque ways that leave the families with little redress against perceived injustice. The degree of surveillance also has a serious impact on family privacy.

2. The current policy in children's services "Every Child Matters" (HM Treasury, 2003) in combination with the Children Act 2004 and Childcare Act 2006 places responsibility on local children's services to improve the well-being of young children in their area and reduce inequalities. This policy is being implemented through the introduction of a range of complex data collection systems which are intended to facilitate the surveillance of children's development and identification of those who need additional help (for full details on the databases see FIPR, 2006). While the aim of helping children is honourable, the means are of concern. The

surveillance of children is being used as a mechanism for social sorting, for classifying children into groups and targeting those deemed "at risk" of some adverse outcome, the main priorities being:

> to reduce the numbers of children who experience educational failure, engage in offending or anti-social behaviour, suffer from ill health, or become teenage parents (HM Treasury, 2003, p.5).

Risk Prediction

3. Surveillance is used to facilitate risk predictions, to screen children and pick out those at high risk. The government have cited the existence of scientific knowledge as a justification for screening children (Blair, 2006a). There is a body of research on factors associated with a range of adverse adult outcomes but this only permits risk predictions with a high level of inaccuracy, of both false positives and false negatives (U.S. Preventive Services Task Force,2004; Farrington, 2006). The harmful effects of false results of either kind need to be studied and there should be public debate about what level of inaccuracy is morally acceptable.

4. How this research is being used in practice is also problematic. In some instances it is being used to create an actuarial risk assessment tool (eg Asset and Onset in youth justice) while in other areas it seems to have no systematic and shared usage; it is not, for example, explicitly referenced in the assessment framework (CAF, discussed below), that most practitioners will be using in judging which children need additional help.

5. The term "pre-delinquent" is now in common use in describing those children who have not misbehaved but who bear many of the risk factors that correlate with delinquency. This usage indicates a misunderstanding of what inferences about the individual are warranted from group statistics.

Quality of the Evidence

6. Besides an inadequate scientific base for computing the probability of adverse outcomes from a set of data, there are problems with the type of evidence used in making the risk assessment since much of it involves subjective judgments. The Common Assessment Framework (CAF) form is a primary mechanism for screening children. It is to be completed by practitioners other than local authority social workers who consider that a child has needs in addition to the universal services:

> It is intended to provide a simple process for a holistic assessment of a child's needs and strengths, taking account of the role of parents, carers and environmental factors on their development. (downloaded from http://www.everychildmatters.gov.uk/deliveringservices/caf/).

7. Some of the required data is factual but many of the boxes that need to be completed require the practitioner to make judgments where there is no objective standard as a reference, eg commenting on the child's positive attitudes, relationships with peers, lifestyle, self-control. Parents are also judged on subjective aspects eg modelling positive behaviour, support for positive activities. The idiosyncratic nature of such judgments poses a problem for parents wishing to challenge their accuracy.

Right to a Fair Hearing

8. The screening processes culminate in identifying some children as at risk of an adverse outcome eg of being a "future menace to society" (Blair, 2006b). Although these judgments are made with the intention of intervening in the child's life in a way that will reduce the risk, they cannot fail to be stigmatising and of concern to the child and parent.

9. Actuarial risk predictions pose problems for families in that they make the judgment opaque even to the practitioners who are using them so it is hard for anyone to fully understand and challenge how the conclusion was reached.

10. The non-actuarial risk predictions pose another set of problems for anyone wishing to challenge them in that they rely on idiosyncratic judgments and intuitive computations of the risk factors.

Privacy

11. The child protection system, responsible for investigating concerns about abuse and neglect, requires information sharing between professionals in order to detect the hidden incidents of abuse and neglect in the knowledge that abusive parents will strive to conceal their wrong-doing. This differs from the situation in relation to children with other problems in their health and development where most parents are concerned for their child's well-being.

12. The degree of data collection required by the new children's policy poses a significant challenge to the privacy of the child and family. The Parliamentary Joint Committee on Human Rights (JCHR) studied the policy and, in its final report, expressed concern that the powers sought by the Government were not proportionate:

> We are concerned that, if the justification for information-sharing about children is that it is always proportionate where the purpose is to identify children who need welfare services, there is no meaningful content left to a child's Article 8 right to privacy and confidentiality in their personal information.

References

Blair A. (2006a) "Our Nation's Future—Social Exclusion" Speech to Joseph Rowntree Foundation, York, 5.9.06. Available from www.pm.gov.uk/output/Page10037.asp.

Blair A. (2006b) BBC News interview, 30.8.06. Available from www.bbc.co.uk.

Farrington D. (2006) "Childhood risk factors and risk-focused prevention". Available from www.pm.gov.uk/output/Page10035.asp.

Foundation for Information Policy Research (2006) *Children's Databases—Safety and Privacy*. Information Commissioner's Office, Wilmslow, Cheshire.

HM Treasury (2003) *Every Child Matters*. The Stationery Office, London.

Joint Committee on Human Rights, 19th Report 2003–04.

U.S. Preventive Services Task Force (2004) *Review of the evidence: Screening children for family violence*, Agency for Healthcare Research and Quality, Rockville, MD. Available from: http://www.ahrq.gov.clinic/3rduspstf/famviolence.

June 2007

Memorandum by Action on Rights for Children (ARCH)

Summary of Submission from ARCH

We apologise for the length of our submission. We feel that this is an important and timely inquiry that gives us an opportunity to air some of the fundamental issues that have troubled us for several years, and we are keen to set out an accurate assessment of the situation as it affects children and their families.

The Government's surveillance and data-collection policy began with children more than seven years ago. We have set out its development chronologically and drawn attention to issues that have significance for the relationship between the State and the individual.

In particular we are concerned about:

- Whether a child may consent in her own right to data collection and sharing, and the elements of "informed consent".
- The change in the relationship between parents and government to one of "partnership" in a child's upbringing.
- The lack of parliamentary time available for adequate scrutiny of legislation.
- The use of secondary legislation to effect incremental change in government powers.

The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State

1. ARCH is a children's rights organisation based on human rights instruments. It has a particular focus on children's civil liberties and on the issues arising from developments in Information Technology.

2. During the past decade, these developments have created unprecedented opportunities for observing children and young people, for supervising and controlling their activities, and for gathering and sharing data about their lives.

3. While manufacturers of commercially-available tracking devices have exploited the marketing opportunities presented by popular concerns about children's safety and health, the government's increasingly actuarial approach to children's development has emphasised the use of IT to monitor and share information about them in an attempt to detect early signs of problems. In-depth profiling tools have been developed that are believed to predict criminality, social exclusion or educational failure on the basis of statistical probability.

4. The position of the private individual who is not interfered with by the State unless he transgresses (or, in the case of children, is at risk of significant harm) is being turned on its head by data collection and surveillance. This has happened without adequate debate and the overall effect on children has been to erode their privacy to a point where it is questionable whether there is now any content to their right to a private and family life.

5. ARCH came into existence in 2001 primarily because of concerns about the new style of school census, and about the Connexions service for 13 to19-year-olds. These two initiatives marked the beginning of a trend towards assessing and monitoring children, and sharing their personal data.

The School Census and National Pupil Database:

6. Section 537 of the Education Act 1996[1] allowed the collection of school-level data but expressly forbade the use of pupils' names. This was amended by the Education Act 1997,[2] and again in 1998[3] to create a statutory gateway requiring schools to provide such "individual pupil information" as the Secretary of State prescribed in regulations. A subsequent series of statutory instruments has increased incrementally the range and quantity of data collected on each child to a point where around 40 separate data items are now taken in a thrice-yearly census, and placed on the National Pupil Database.

7. This significant shift from the collection of school performance data to the collection of a large quantity of individual pupil data was achieved via an amendment to the Education Act contained in the 30th schedule to the (lengthy) School Standards and Framework Act 1998. Provisions allowing that pupil data to be shared were introduced as a government amendment to the Bill at the final (21st) session of the Commons Committee Stage, when the Rt Hon Theresa May MP remarked that it: "replaces two lines of schedule 28 with 71 lines of text."[4] We do not believe that the far-reaching powers given to the Secretary of State have ever received adequate parliamentary scrutiny.

The Connexions service:

8. The Learning and Skills Act 2000 paved the way for the Government's "Connexions" service for 13 to 19-year-olds, designed to identify any problems experienced by teenagers that might present "barriers to learning". ss117-120 place a duty upon "learning institutions" to supply any information in their possession about a pupil to the Secretary of State, and provide for widespread information-sharing between public bodies. Information received from learning institutions is used by the Connexions service to identify all those aged 13 to 19, and each young person is allocated a 'Personal Adviser' (PA) whose role is to carry out a personal assessment and to broker access to services.

9. During its passage through Parliament, the privacy implications of the Learning and Skills Act were not debated. At committee stage in the House of Lords, Baroness Blatch asked whether the information-sharing proposals raised data protection issues, and was assured by government that the Data Protection Act would be fully complied with. The issue was not raised at committee stage in the House of Commons. A member of the Standing Committee with whom we subsequently discussed the privacy implications of the Act told us that the quantity of new legislation and consequent pressures on parliamentary time were making effective scrutiny of bills increasingly difficult.

"Every Child Matters":

10. Connexions can be seen as a prototype for the more recent development of the "Every Child Matters" (ECM) agenda, outlined in the green paper of that name in 2003.[5] This extends to all children the idea of gathering and sharing information between agencies in order to identify signs of problems and intervene at an early stage.

[1] s537 Education Act 1996: http://www.opsi.gov.uk/acts/acts1996/96056-cl.htm#537
[2] s20 Education Act 1997: http://www.opsi.gov.uk/ACTS/acts1997/97044--g.htm
[3] schedule 30 para.153 School Standards and Framework Act 1998: http://www.opsi.gov.uk/ACTS/acts1998/80031ccd.htm
[4] NB Schedule 28 subsequently became Schedule 30. HofC Standing Cttee A: http://www.publications.parliament.uk/pa/cm199798/cmstand/a/st980303/pm/80303s02.htm
[5] DfES "Every Child Matters" (2003) http://www.everychildmatters.gov.uk/_files/EBE7EEAC90382663E0D5BBF24C99A7AC.pdf

11. Every Child Matters sets out five outcomes for each child: being healthy; staying safe; enjoying and achieving; making a positive contribution; achieving economic wellbeing. Responsibility for the achievement of these outcomes has been given to local authority and health agencies, reconfigured into Children's Trusts, which have been given 26 Public Service Agreement targets (PSAs) and 13 Key Indicators[6] against which to measure their performance.

12. ECM was given effect by the Children Act 2004, s12[7] of which empowers the Secretary of State by regulations to make provision for the establishment and operation of database(s) and variously requires or permits the sharing of information between practitioners "… notwithstanding any rule of common law which prohibits or restricts the disclosure of information". Two parallel database systems are now being developed.

ContactPoint:

13. The first of these databases is a national system, piloted as the "Information Sharing Index" and now re-branded as "ContactPoint". It is envisaged that this will hold identifying information about each child from birth to 18, plus contact details for all services that he is using (although details of involvement with substance abuse, sexual and mental health services will normally be hidden). Following parliamentary debate, the government agreed that regulations specifying the data to be collected and the manner in which it would be displayed should be subject to the affirmative resolution of both Houses. The rules governing access to the data, and the operation and security of the database, will be set out in guidance.

Common Assessment Framework (eCAF):

14. The "Common Assessment Framework" is being developed by each local authority, to be used by any practitioner other than specialist social care staff who believes that a child is not progressing towards the "five outcomes", or needs additional services. It is an in-depth, personal profiling tool that explores every area of a child's life and development. The government estimates that around one-third of the child population is in need of additional services at any given time.

15. The CAF practitioner's guide[8] gives a six-page list of the assessment criteria, and although practitioners are advised that they should base their assessment on evidence, several of the areas covered require the practitioner to form an opinion on abstract issues such as the quality of children's relationships and the capabilities of their parents.

Youth Justice:

16. The emphasis given to early assessment and intervention by ECM echoes a risk-management approach to children that has also developed in the youth justice sector. Certain factors are believed to be predictive of future offending behaviour, and a number of assessment schemes and prevention projects exist to divert those believed to be "at risk" of committing offences. One such scheme requires Youth Offending Teams to identify the 50 children in its locality thought most likely to offend.[9]

The National DNA Database (NDNAD):

17. It has recently been estimated that, at a minimum, the DNA profiles of 100,000 children who have not committed any offence are held on NDNAD. This potentially places these children under suspicion whenever a positive DNA match is made at a crime scene. Given that the police may also access the other information outlined above, and will certainly be able to see from ContactPoint that a child is involved in a youth justice diversionary programme, we are concerned that a set of assumptions could be created that will influence police attitudes, including the likelihood of guilt.

[6] Every Child Matters Outcomes Framework: http://www.everychildmatters.gov.uk/_files/F25F66D29D852A2D443C22771084BDE4.pdf
[7] The Children Act 2004 s12: http://www.opsi.gov.uk/acts/acts2004/40031--c.htm#12
[8] *HM Government The Common Assessment Framework for children and young people: Practitioners' guide* (Annex A: Definitions): http://www.everychildmatters.gov.uk/_files/A19154AA073AF2F7216B25A693916CF6.pdf
[9] Youth Justice Board: "ID50-guidance for partners" http://www.yjb.gov.uk/NR/rdonlyres/0233E9E7-8E58-45E0-ACF8-E3190B8EAD19/0/ID50guidancedocumentforpartners.doc

Consent:

18. A key issue with all of the existing and proposed database systems is that of gaining the consent of those to whom the information refers. It is accepted that information can and should be shared without consent when a child is at risk of significant harm but, particularly in the youth justice sector, the threshold is often far lower than this and refusal to consent may in any case be overridden by reliance on a general, discretionary duty to prevent crime. YJB guidance on sharing information to identify those thought to be potential young offenders advises that: "obtaining consent remains a matter of good practice, as opposed to a requirement of law".[10]

19. The situation is further complicated by the issue of when an older child can give consent in her own right. Settled law established in *Gillick v West Norfolk and Wisbech Area Health Authority*[11] provides an exception to the common law principle that parents are responsible for their under-age children, but the strict guidelines laid down by Lord Fraser, who gave the leading speech, include the proviso that a child must actively refuse parental involvement when her "informed consent" is sought. This is now routinely misrepresented as a need to consult parents only when a child is not competent to consent.

20. A child may not feel able to insist that her parents be involved. She may feel under pressure to consent to information sharing if she believes that she must concur with adults' wishes in order to access services or to avoid trouble. Any presumption in favour of excluding parents from the decision-making process also risks breaching the child's right under Article 5 of the UN Convention on the Rights of the Child to seek guidance from her parents.

21. When a child is seeking access to a specific service, there is an assumption that a practitioner with relevant, specialist knowledge will offer detailed and unbiased information upon which a child can rely in reaching a decision. We would suggest that the only type of practitioner able to provide sufficient information to enable a child to give genuinely informed consent on data storage and sharing is one with specialist knowledge of the subject, and an appreciation of the use to which data might be put in the future. We would add that the emphasis placed by government on the need for information sharing inevitably creates an institutional bias towards gaining consent.

22. While it is important that a child or young person can seek help and advice in confidence, and may be perfectly capable of consenting to counselling or medical treatment, this is not the same as being competent to understand the full implications of complex and/or ongoing acts of data-sharing. This data may not only be about the child herself. The practitioner guidance to the CAF[12] advises that:

> Opinions should be recorded and marked accordingly (for example "Michael said he thinks his dad is an alcoholic").

Unless there are genuine child protection concerns, in our view such information should not be recorded without the consent of the person to whom it refers.

23. We cannot offer an easy solution to the difficulties surrounding the consent of older children to data storage and sharing. It is important that children themselves have some control over their personal information and that when they have properly been assessed as Gillick competent in obtaining a service, their confidentiality is maintained; it is equally important that parents are not relegated to the status of junior partner in their child's upbringing and that they retain the protective function provided by Article 5 of the UNCRC.

24. This complex area has not been debated at all. In our view, the government has fudged the issue by simply ignoring one of the central rules set out by Lord Fraser in the *Gillick* case, and his warning that the judgment:

> . . . ought not to be regarded as a licence for doctors to disregard the wishes of parents on this matter whenever they find it convenient to do so. Any doctor who behaves in such a way would be failing to discharge his professional responsibilities, and I would expect him to be disciplined by his own professional body accordingly.[13]

We are therefore concerned about the basis for the Government's assertion that:

> In most cases, where a child cannot consent or where you have judged that they are not competent to consent, a person with parental responsibility should be asked to consent on behalf of the child.[14]

In our view, the issues surrounding children's "informed consent" need urgent scrutiny and debate.

[10] Youth Justice Board, "Sharing Information on Children and Young People at Risk of Offending: A Practical Guide" www.youth-justice-board.gov.uk/Publications/Scripts/fileDownload.asp?file=infosharing0305.pdf
[11] *Gillick v West Norfolk and Wisbech Area Health Authority* [1985] 3 All ER 402
[12] HM Government The Common Assessment Framework for children and young people *Op cit*
[13] *Gillick v West Norfolk and Wisbech AHA op cit*
[14] DfES Information Sharing: Practitioners' guide (2006) http://www.everychildmatters.gov.uk/_files/ACB1BA35C20D4C42A1FE6F9133A7C614.pdf

Legislation

25. Over the past few years we have becoming increasingly concerned about the lack of time available for legislative scrutiny of Bills. We can think of several occasions where the final clauses and schedules to a Bill—and government amendments to them—have simply been "nodded through" in the closing stages of committee debate. The problem is compounded when controversial proposals that affect the relationship between the individual and the State are contained in the latter part of a Bill, or are masked by more overt controversies. Unless the quantity of legislation that a government can introduce in any session of parliament is restricted in some way, this problem can only get worse. How can a single MP or Peer be expected to master the entire content of several lengthy Bills?

26. It is unusual to find any power that governs surveillance clearly set out on the face of a Bill. When the Children Act 2004, for example, was first introduced to Parliament, it resembled a blank cheque in that it contained a series of provisions for the Secretary of State to prescribe the content and governance of children's databases in regulations. It was only after intense lobbying and parliamentary pressure that the data items were specified on the face of the Bill and agreement reached that regulations would be subject to affirmative resolution. There still remains a power at s12(4)(h) for the Secretary of State to vary the data that is collected.

27. This use of primary legislation as a gateway to create governance through secondary legislation creates a climate inherently favourable to "function creep" because governments can increase their powers with very little scrutiny—as the school census demonstrates. We would suggest that it is essential to return to an assumption that a government's powers are normally set out in primary legislation.

28. There have been several occasions when an apparent lack of compatibility of a Bill's provisions with the Data Protection Act or Human Rights Act has been raised in Parliament, and the government has dealt with this by stating that it is incumbent upon any public authority to ensure compliance. The legislation itself should only specify powers that are compatible with the ECHR and DPA and not abrogate the responsibility to those carrying out functions under the legislation.

The relationship between the State and the family:

29. The "Every Child Matters" agenda is predicated upon an idea that the State works in "partnership" with parents in the upbringing of children. New guidance entitled "Every Parent Matters" says that:

> The role of government is to ensure that all parents . . . work in partnership with services to reinforce the benefits for their children's outcomes.[15]

Parents have at no point been asked their views on the role of State agencies as partners rather than public servants, nor have children expressed any wish to have responsibility for their upbringing shared between their parents and government.

30. Certainly there is a role for the State in intervening to prevent significant harm from abuse and neglect, enshrined in s47 of the Children Act 1989. Some may argue that not encouraging education or not giving a child sufficient fruit and vegetables are forms of neglect; however, if the boundaries of legitimate state intervention are drawn so widely, not only are the small number of children genuinely at risk of significant harm likely to be overlooked in a welter of low-level information, but serious questions are also raised as to who is actually bringing a child up. The main thrust of all human rights instruments is to support the integrity of families and the role of parents in their child's upbringing. Government policy appears to diminish that role.

31. Responsibility for the five outcomes in "Every Child Matters" is given to local Children's Trusts. Through the PSA targets, they are charged with ensuring that children take up sporting opportunities or consider running their own businesses; that they do not smoke or become offenders, and that:

> The progress of individual children and young people in educational, personal, social and emotional outcomes is regularly reviewed and communicated between agencies, and targets revised accordingly[16]

32. Although the State's role in "supporting" parents is repeatedly emphasised, the very existence of government targets for every aspect of a child's development, given close definition by the PSA targets, means that such support is inevitably aimed at encouraging parents to assist in the achievement of the five outcomes in a manner prescribed by government.

[15] Para 2.6 "Every Parent Matters" DfES (2007) http://www.teachernet.gov.uk/_doc/11184/6937_DFES_Every_Parent_Matters_FINAL_PDF_as_published_130307

[16] Every Child Matters Outcome Framework *op cit*

33. There appears to be no room for a parent or child to decline the offer of services, nor to disagree with "experts" (indeed such disagreement can itself be grounds for concern). When faced with several practitioners presenting a united front, it may be especially difficult to withstand pressure to conform. It is hard to see how a target-driven child-development template allows any space for eccentricity or for the highly unconventional family within which children are nevertheless raised with dignity and love.

34. We welcome the Constitution Committee's inquiry, and hope that the matters we have set out above will be of assistance. We would be pleased to help further in any way that we can.

8 June 2007

Examination of Witnesses

Witnesses: Ms Terri Dowty, Director, Action on Rights for Children (ARCH), Dr Eileen Munro, Reader in Social Policy, London School of Economics and Political Science, examined.

Q810 ***Chairman:*** Perhaps I could begin. Action on Rights for Children is generally critical, as I understand it, of the collection of children's personal data and its use in sharing or in other ways to reduce both the risks to children and the threats that certain children may pose to the wider community. How should we strike the balance between the need to protect people and the need to respect children's privacy?

Ms Dowty: First of all, we need to be clear about what we mean when we talk about risk. We need to make clear distinctions between child welfare and child protection. The Government has expanded the definition of "at risk" from its generally accepted meaning, taken from section 1 of the Children Act 1989 of "at risk of significant harm from neglect or abuse" to cover all kinds of other situations: at risk of teenage pregnancy; at risk of abusing substances; at risk of becoming a criminal. This blurring of the definitions, this rather loose use of the phrase "at risk", has led many people to believe that the Government's *Every Child Matters Agenda* is about child protection, that it is about children at risk of harm, when in fact it is about the estimated 50 per cent of children by the Government's estimation who will at some point need access to services in order to help them achieve the five outcomes that the Government has established in the *Every Child Matters:* be healthy; stay safe; enjoy and achieve; achieve economic independence; and make a positive contribution. There is a world of a difference, though, between a child in need of services who has capable, concerned parents, and the child who is in danger from their parents or whose parents are not able to meet their vital needs. We get into dangerous territory when we start confusing these two categories of children. In the first case, there is no reason to suppose the parents and the family themselves are not capable of deciding what services they need and asking for them for themselves, in which case it is the Government's function to see that those services are available and that they are properly resourced and properly staffed. In the second case, the Government has a legitimate duty to intervene where parents are failing to be good parents to their children. This loose language is also a problem when we talk about youth justice and whether children are a risk to other people or not. It depends how you define the threat. Are we talking about children who are annoying? A group of teenagers hanging around being very noisy on the estate may be thoroughly annoying, but are they a threat to anybody? Some people may feel threatened. Should they feel threatened, or is it they who are being unrealistic about it? I think it would be easier to strike the right balance if we had grounded the *Every Child Matters* agenda solidly in the UN Convention on the Rights of the Child. There is a real problem here: the Government believes that its five outcomes manage to capture the UN Convention on the Rights of the Child, which I find a worrying claim. I am not quite sure how you encapsulate all those articles in five short statements. Also, it excludes all children's civil rights: the right to freedom of association; the right to privacy –which is fundamental to a child's development, in my view—and it also excludes mention of a child's right to be guided by their parents, and of the role of government in promoting respect within society for the role of parents. The Convention taken as a whole provides a series of checks and balances against over-enthusiastic state intervention and those are simply not there in the five outcomes. It also gives us the "best interest" principle: that anything done must be in the best interests of a child, but unless you locate best interest securely with the framework of the Convention, there is a risk that the best interests of the child become a rather more vague "what is good for children generally" and not about the individual child, and it is also a licence for practitioner bias as to what is right for a child rather than what that child's rights are.

Q811 ***Baroness O'Cathain:*** Do you think that government has reached too quickly for databases and information technology solutions to problems such as child abuse and neglect, overlooking other approaches involving the exercise of traditional professional judgment?

Ms Dowty: Perhaps I could ask Eileen to answer that one.

Dr Munro: My particular expertise is in child protection, so I am very aware of the problems there in terms of information sharing. If you think about the process of sharing information, you first of all have to recognise that you have a piece of information that could be a signal that there is abuse in the family; second, you need to know who to send it to and how to send it to them; and third, that other person has to receive and understand it. When you look at the errors that happen in child abuse, it is around people not recognising that a signal of abuse is abuse, or sending it and the other person not receiving it. In Victoria Climbiéøs case, for instance, the hospital sent a medical report and it was not read, and when they had supervision they did not take the social work record into the room with them. The problems do not arise in the technical sending of data but in the understanding of data. We have excellent working together procedures that have been in place since the 1970s and are very well known and very clear.

Q812 ***Lord Peston:*** I understand your points, Dr Munro, on abuse and all that, but I would like to take us back to the first question about correct behaviour, the converse of abuse, forgetting the old joke that we are all too young when we are bringing our children up and it is only when many years go by that you realise how you ought to have brought them up. God knows when the UN got itself involved in all this, because certainly when we were bringing our children up—I am sure completely hopelessly—it would never have occurred to us that it was other than our responsibility. One of my questions to both of you is: When did all this change, this notion of, if you like, the philosophical concepts of rights and all that? The particular one I totally agree with you about is the right to privacy. It seems to me that children have their own lives. I did not know that when I was bringing my children up. I should have known, because I remember not telling my own parents about my private life, but it never occurred to me that my children had any secrets from me! Some of the secrets really mattered to them. The fact that we made our children wear Marks & Spencer's clothes they thought was absolutely appalling behaviour, and they might have gone to you, Dr Munro, saying, "This is real child abuse."
Dr Munro: I would have agreed with them, yes.

Q813 ***Lord Peston:*** "We want to be clothed from the charity shop like all our friends." Can you give us a perspective on this more than we have had?
Dr Munro: There is a strong British tradition of the family having privacy for centuries. It was at the very end of the 19th century that you got the first piece of legislation against child cruelty and it was specifically against the severe end, of severe physical chastisement or extreme neglect—starvation levels—but then it was really in the 1970s that you got an escalation. Before the 1970s we basically had a child welfare service, with a bit of abuse every now and again, but families were generally seen as problem families or families with problems but the language of child protection came in in the 1980s and then the language of safeguarding children to ensure that they have an ideal childhood came in under the 2004 Act. The idea of going from family privacy to at least caring about dangerous and malicious parents and then to wanting to monitor and ensure all children are reaching some standard of experience is very recent.

Q814 ***Lord Peston:*** We never struck our children at all. It would never have occurred to us that that would be other than a failure on our part. But there are plenty of perfectly decent parents who feel the reverse. I am never quite clear: is that a matter of rights, children versus parents or what?
Dr Munro: It is pragmatic as well, but it is not a very effective way of disciplining.

Q815 ***Lord Peston:*** I agree with you entirely.
Dr Munro: So there is that argument. As somebody interested in child protection, I do not get very bothered by a slap. It is much more serious injuries that worry me. But it basically is that it is an ineffective way of discipline and it is offensive to children and they are deeply distressed by it. The right to their being treated reasonably well does protect them from it, I think.

Q816 ***Lord Lyell Markyate:*** Dr Munro, first of all, thank you for a very, very interesting paper. Can you explain why the Government have added a concern for broader goals of child welfare and protecting society to their traditional concern of protecting children from harm? What do you see as the implications for children as citizens of in-depth profiling tools for predicting criminality, social exclusion, or educational failure on the basis of statistical probability, which you mentioned in your written evidence and in the FIPR report for the Information Commissioner? I know I am asking you, in a sense, to rehearse what is in your paper, but it would be very helpful for us if you could talk about the key points.
Dr Munro: I have no objections to the Government expressing concern that children have a decent childhood. The aim of the policy is not one I want to criticise; it is the means of doing so which is, to my mind, taking away too much responsibility from parents for deciding what their children need and what their goals and priorities in life should be. I do not want in any way to object to welfare services being available, to parenting classes being around if

parents want to go to them, but the Government are seeking, I think mainly on economic grounds, to target the families that most need the help via profiling. Economically this would make sense if you could do accurate profiling with no detrimental effect on families, but when you look at the probability theory and the kind of knowledge we have, if you are looking at a very specific risk, a risk of being abused or a risk of being a criminal or a risk of doing badly at school, any specific risk instrument will have a very high inaccuracy rate. When you do the Government's process of putting the whole lot together in a job lot, then the risk assessment is incredibly bizarre and the level of false positives and false negatives is extremely high, and the impact upon a child and family of having a false positive ascribed to them is very destructive—and it is unjust.

Q817 ***Lord Lyell of Markyate:*** I remember once doing a child protection case—and we are going right back into the 1970s—and I still squirm at myself, at the amount of hearsay evidence of a pretty dubious and inaccurate basis which I put forward to the court. I am glad to say it was overturned when it got to the Crown Court—and that shows how long ago it was. There is another member of this House, Lord Temple-Morris, who won the case against me. What you have said is not new but it is terribly important: that it is very easy to build up a false and dangerous case.

Ms Dowty: That danger is exacerbated by the kinds of criteria that are being used to assess whether a child is at risk of becoming criminal. When you look at the criteria on things like the RYOGENS system or that are used in onset, the criteria are things like being on a low income, living in poor housing, having a lack of facilities. They are problems of poverty, and it is rather insulting immediately to assume that because somebody is poor they are going to turn out to be a criminal. We know from the evidence from people like Professor Farrington at Cambridge University, for example, that there is a lot to be said for targeting resources at deprived areas and it does have an effect in improving education standards and reducing delinquency, but to go from that to saying that you can find an individual who is likely to become a criminal is described by Professor Farrington as "fanciful"—and I know a lot of people have been less polite than that about the idea.

Q818 ***Baroness Quin:*** I totally share the concerns about inaccurate information and, also, indeed, out-of-date information which might unfairly stigmatise someone subsequently. Dr Munro, I have read your paper and I wonder what the alternative is in terms of trying to ensure as much support and helpful intervention for a large number of areas of dysfunctional families where children are extremely vulnerable.

Dr Munro: I think we should start with the assumption that parents are responsible until they have proven to have reason for us to doubt it. The fact that they are poor should not in itself mean that they are vulnerable to scrutiny by welfare services as feckless and dodgy parents. I would be delighted to see more services available, particularly mental health services for children and for adults, but it is about how they are provided. It is about whether you make them available, tell parents about them, tell them what they can do and what they cannot do, and make it attractive for parents to want to use them. Most parents do care very deeply about the well-being of their children and they almost certainly care about it more than any teacher or police officer does. It is a question of providing the services but not saying that the state will decide who is a defective parent and we will decide what help you need to rectify it, except at the extremes of: "That is definitely bad parenting and we must intervene whether you like it or not." There is no right way of bringing up children. There are some very definitely bad ways. In terms of prescribing any set right way, there is not scientific evidence for it and the reality is that most of us muddle through quite well while doing different things.

Q819 ***Lord Peston:*** The distinction you make on the statistical analysis is a standard problem for social scientists. We are very good at saying "on average" or "this cause will have that effect" but that does not identify any individuals. But in the end our concern is that we somehow have to get to the individuals. What troubles me, again thinking back to bringing up my own children or, even worse, my own grandchild, is that they have every advantage. I do not mean that we are tremendously rich but they have two parents there all the time rather than one, they are being bombarded all the time with "Have you read this, have you done that" and so on and so forth. In a competitive world, I constantly say to myself, "What chance do quite a lot of other children have?" I am not clear how you go from one to the other. I take your point about directing resources, but it is more than that. My daughter as a personal social work theme would find those girls at the local comprehensive who could not read and teach them to read, but it was always two steps forward and one step back because at home there was not the pressure that she had at home of "What have you learned today?" but totally different pressures. I am not very clear what our duty is in terms of response here. Can you elucidate that? In the end, each of us surely agrees that what matters to you is the individual child.

Ms Dowty: Yes, it is the individual child, and it is also about the family that is bringing them up. That is where I think there is a real danger that we impose our ideas of what a good childhood is and what a good outcome is, of what people should be achieving through their education. It is for families to bring their children up and for the state to make sure services are available, properly funded, and that we have good schools that are not failing and where children can achieve if they want to. Something that has been ignored in the debate around this change towards information sharing and profiling is that services are not available. The Commission for Social Care Inspection reported last year that the threshold for receiving the most blatantly obviously necessary services, like disability aids and so on, are climbing and climbing, so it is very hard for families to access basic care. We have a huge shortage of midwives, a huge shortage of health visitors. We have had an ongoing chronic shortage of child and family social workers now for several years. I do not know how long it has been going on but we are around 2,000 to 3,000 short on child and family social workers. If you do not put the services in place, then you are not going to get anywhere, but let us try having the services in place and then seeing how parents get on with bringing up their children.

Q820 ***Lord Rowlands:*** I am slightly bridling at some of the things you are saying. It is not that we are imposing our views of childhood on others. Over 30 years of constituency case experience taught me repeatedly that the problems with childhood were mostly the problems of parents—and although I use the word in plural, in many cases there were not parents, there was a parent, at best, and probably more likely a grandma rather than even a mother or a father. It did not seem to me very difficult to identify those children as vulnerable and needing all the support they can get. They are a minority of cases. If we have a wonderful, romantic view of family in certain circumstances, we will get it wrong and we will end up with those children in fact being more vulnerable and failing, and possibly drifting into crime of one kind or another. I do not think we can be as starry-eyed as perhaps your evidence has suggested.
Ms Dowty: I do not think I am starry-eyed at all. Yes, you are right, there are children who are struggling and they do need some kind of intervention, and, as you have said, they are a small minority of children. With the Common Assessment Framework and the profiling that is going on, the Government are talking about 50 per cent of children needing to have the profiling carried out. That is the problem: at some point we stray across and intervene with parenting.

Dr Munro: You said that they were easy to identify, so we do not need a national database and a national electronic CAF and all of this surveillance if they are already identified.

Q821 ***Lord Rowlands:*** But what you do need, if I might say so—and I felt it often as a Member of Parliament—is more information about that young person. I worked with a charity training young people who in many cases have failed school or are dysfunctional and one could do much more if you did know more about what had happened to them. That means you do need some kind of data and you do need some kind of data sharing.
Dr Munro: It needs a professional with the time to go and read the information and with the wisdom to make sense of it. The problems lie at that point in the system rather than having some kind of technical data around, because if nobody is able to pull all the pieces together into a decent assessment—

Q822 ***Lord Rowlands:*** That requires data sharing to do that.
Dr Munro: The kinds of families you are talking about really fall into the child protection system, because you are talking about a serious level of neglect, that the child is not getting adequate parenting.

Q823 ***Lord Rowlands:*** They are not being abused in the physical sense.
Dr Munro: No, but this is neglect in the sense of not having their needs met.

Q824 ***Lord Rowlands:*** Yes.
Dr Munro: We already have that system in place, and the fact that they are not getting picked up by it is more because of that system being overloaded—but it does exist. It is a different category of problem from the parent who is looking after a child with disabilities, who is struggling and asking for more help.

Q825 ***Lord Woolf:*** There are undoubtedly a very large number of databases. There are other methods of sharing information which has been collected. What is your view concerning the legality and consents needed for those activities?
Ms Dowty: There is a huge problem at the moment around consent to data sharing. There are, I should say, article 8 problems, I believe—article 8 of the European Convention on Human Rights—with at least some of the databases to which the Joint Committee on Human Rights drew attention when the Bill was going through Parliament, pointing out that it did not seem to be a proportionate response to share information on all the children in order to identify those who might need welfare services. But

key to the whole issue of confidentiality and privacy is that of consent. I have seen, just in the last year or so, three different sets of advice on consent in three different sets of government guidance, so we have the Youth Justice Board operating what is called the ID50 scheme, where a local authority has to identify the 50 children considered most likely to become offenders within the local authority area. In the ID50 guidance the Youth Justice Board says that gaining consent is a matter of good practice rather than a matter of law in order to share information about these children. The Government's guidance to the Common Assessment Framework says that a child of around 12 and perhaps even younger is competent to consent to data sharing, but the legal basis for that is unclear. The information sharing guidance that the Government issued, on the other hand, says that parents should always be involved in any decision. Unsurprisingly, practitioners are very confused, and it really is not clear what is happening. We have been funded by the Nuffield Foundation for the rest of this year to conduct a study of the law relating to children's informed consent. I am having quite an interesting time at the moment talking to senior legal academics and practising lawyers to try to tease out exactly what the black-letter law is about children and consent and I hope that I will be able to bring more clarity to the current debate by the end of this year when we publish the report.

Q826 ***Lord Woolf:*** Is this an area where you feel the Information Commissioner should be providing guidance? In so far as that is being done now, do you think it is sufficient?
Ms Dowty: No, I do not think it is. On the issue of consent, I have been talking to the Information Commissioner recently and they also are using the age of 12 as a suitable age to gain subject access to records, because of the *Gillick* case. But if we are going to use the *Gillick* case, we have to use the whole judgment, not cherry-pick—

Q827 ***Lord Woolf:*** "Judgments" in the plural.
Ms Dowty: Judgments, yes, rather than leave out important elements that Lord Fraser outlined in the process of getting the child's consent. It is just such a confusing area that I do not think the Information Commissioner has been any help, to be honest.

Q828 ***Lord Woolf:*** Guidance is definitely needed, in your view. Do you hope you are going to be able to provide that?
Ms Dowty: I hope I might be able to persuade people either to apply the law correctly or that it is time that Parliament looked again at the issue of children's consent. The last time Parliament looked at it was in 1969 in the Family Law Reform Act. Since then, all kinds of things have happened: we have had the Data Protection Act; we have ratified the Convention on the Rights of the Child; we have had the Human Rights Act. All sorts of things have changed. We have had various judgments. Perhaps it is time that Parliament looked at the age of legal capacity.

Q829 ***Lord Woolf:*** How well, in regard to what you say, does what I believe is the technical term "ContactPoint" fit into this?
Ms Dowty: ContactPoint is a central identity index of children. It is an identity management database, combined with a directory that will bring together all of the agency systems around the edge. It provides a central hub to put practitioners in touch with each other, so that they can share information directly, because all systems are now built to a mandatory interoperability specification.

Q830 ***Baroness Quin:*** I am just wondering if you have had contact with the Children's Commissioner over your concerns, and what the reaction has been both in England and in other parts of the UK.
Ms Dowty: Yes, we have had contact with all the Commissioners. As an organisation we have regular contact with Commissioners anyway and when we were doing the FIPR report we certainly interviewed them and kept them in close touch. Amongst all of them there was genuine worry about the move towards data sharing without proper consent and the fact that there was this lack of clarity that should have been dealt with before the agenda was fully formulated. There was concern about the interference with children's rights to have the guidance of their parents when they are making decisions about the exercise of their rights and this sidelining.

Q831 ***Lord Rowlands:*** I read with great interest in the written evidence the criticism you made of lack of parliamentary scrutiny of legislation which extends these databases and data sharing. You are also quite critical of excessive secondary legislation which has promoted databases and sharing. Do you have any thoughts about how we might address the issue? Do you think we need a new kind of parliamentary procedure to address it?
Ms Dowty: Yes. If the trend is going to continue for using primary legislation to create coat-hooks for secondary legislation, then we are shifting—

Q832 ***Lord Rowlands:*** Which is what that decision does anyway.
Ms Dowty: Yes, but we are shifting our legislation to the executive, effectively, in relying so heavily on secondary legislation, and I think there needs to be greater scrutiny.

Q833 ***Lord Rowlands:*** Could you give me an illustration of the secondary legislation which has done this, which has promoted or extended databases, which one would not have spotted in the primary legislation.
Ms Dowty: The classic example was the National Pupil Database. Originally contained in the Education Act 1997 there was the provision to collect information from schools on an aggregate basis in order to plan for services. Into the School Standards and Framework Act, in something like the 29th or 30th schedule, there was inserted an amendment, halfway through committee stage, that turned that into a power to share individual information about pupils and to specify that information in regulations. Since then, we have seen a classic example of function creep, because the school census is now termly and they have gone from collecting very basic information about children to quite detailed information, including how a child gets to school in the mornings, recording behaviour and attendance data, whether they have special needs and whether they have free school meals. This is all going on to the National Pupil Database, which is, as far as we know at the moment, a permanent database without the intention to delete the content of it. That is a perfect example of a power that got through with little scrutiny because at the time there was not the same awareness of the power of databases and of information sharing.

Q834 ***Lord Rowlands:*** I notice you quoted the 2000 Learning and Skills Act. An Education Bill that had its second reading here yesterday also has considerable provision about data sharing, does it not?
Ms Dowty: Yes, it does.

Q835 ***Lord Rowlands:*** Have you scrutinised that? Have you thought about that?
Ms Dowty: We have thought about it a great deal. We are so over-committed with work at the moment that we have not been able to focus on it, but the Children's Rights Alliance and an alliance of various other charities I know are dealing with it, and we have been giving them advice on that.

Q836 ***Lord Rowlands:*** One idea that has been floated—and we floated it ourselves in the previous hearing—is that we should have some sort of mandatory privacy impact assessment on legislation, so that, before a department brings a bill forward—just like it has to do on human rights—where there is any element of data sharing involved there has to be a privacy impact assessment in which the department has assessed the consequences of that data sharing in terms of privacy. Would you welcome that kind of approach?
Ms Dowty: Yes, we certainly would. It is a way of making legislators think about what they are doing.

Q837 ***Lord Rowlands:*** It is being aware.
Ms Dowty: It is being aware of the privacy issues that can arise. I also wonder if it would not be helpful to introduce a committee stage for regulations that are subject to affirmative resolution, so that we extend the process.

Q838 ***Lord Rowlands:*** That is the secondary legislation you referred to.
Ms Dowty: Yes. I am thinking about the regulations that are bringing ContactPoint into being, for instance. You cannot amend the regulations and it is unlikely that they are going to be rejected, but if we are going to give the executive such far reaching powers to create legislation then perhaps there needs to be a process whereby things deemed sufficiently serious to warrant affirmative resolution actually receive proper scrutiny by committee and perhaps introduce the opportunity to amend regulations at that stage.

Q839 ***Lord Lyell of Markyate:*** Lady Quin was asking, quite rightly, what should we do. Looking at your warning of 22 November 2006, the FIPR warning, what you are really saying is that we simply must not extend all this ill-digested information because it is likely to do significantly more harm than good. Is that what you are saying? Is that still true now, 18 months, nearly two years later?
Dr Munro: Yes. I think you also need to remember that people who provide services with good intentions do not necessarily produce good outcomes for the children. There is growing evidence that the early intervention services are not only failing to be as effective as the Government hoped but there is some evidence of them doing harm. In the Sure Start schemes, the most disadvantaged families did worse in the Sure Start areas than in the control areas. The efforts to identify and treat children who might become delinquent has not been successful but has increased the number of those children going into the juvenile justice system. It is not just the data sharing. Good intentioned people can do bad things.

Q840 ***Lord Morris of Aberavon:*** I want to ask you about the Data Protection Act. Does it provide sufficient safeguards for the privacy issues arising from the use of these databases?
Ms Dowty: No, it does not. It is a very short answer really. So long as the Government legislates by creating statutory gateways that override the need for consent in the Data Protection Act, and so long as that is allowed to happen repeatedly, then the Data Protection Act offers no protection at all. At the

moment information can be shared without consent if there is a statutory duty upon a body to share information. We have seen cases where the Data Protection Act would not allow the sharing of information and so the Government have simply created legislation that places a statutory duty, and suddenly the Data Protection Act is worthless, if that makes sense. There is also the issue of the use of broad discretionary powers to allow the sharing of the information. The Data Protection Act does not appear to limit those powers, so we have, for instance, information shared on the basis of a general duty on a local authority to prevent crime in their area or to reduce youth offending. That is then used to justify specific instances of information sharing about an individual. Suddenly the line becomes very blurred. How far do we go to stop crime occurring in an area? Does this broad power allow the police to enter your house and search for stolen goods? Presumably not. Why does it allow information to be shared, but it seems the Data Protection Act does not stop that?

Chairman: Ms Dowty and Dr Munro, may I thank you on behalf of the Committee very much indeed for being with us and for the evidence you have given us. Thank you very much indeed.

WEDNESDAY 18 JUNE 2008

Present	Goodlad, L (Chairman)	Quin, B
	Lyell of Markyate, L	Rodgers of Quarry Bank, L
	Morris of Aberavon, L	Rowlands, L
	Norton of Louth, L	Smith of Clifton, L
	Peston, L	

Memorandum by Dr C N M Pounder, Editor of Data Protection and Privacy Practice

Introduction

1. This evidence is limited to exploring two of the issues identified in the Committee's press release associated with the launch of its investigation: "To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?"; and "Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?".

The Need for a New Kind of Parliamentary Scrutiny?

2. The current mechanism of Parliamentary scrutiny has resulted in the following problems:

(a) Approval of widely drawn powers[1] which in the context of surveillance exacerbates the risk of function creep or the use of powers by a future Government in a different context. For example, 30-year-old, wide-ranging powers are used to justify vast tracts of data sharing or data access[2] by the Inland Revenue. It is therefore arguable that it is unsafe to leave broad powers on the statute book and that approval of certain powers should be refreshed by Parliament (eg every 10 years). The Information Commissioner could be given the obligation to recommend to Parliament which powers should be refreshed.

(b) The Government is in a unique position as it can enact legislation or use existing powers to modify the impact of all the Data Protection Principles in order to meet its processing objectives, and in data protection terms, this ability can degrade the protection afforded by the most Principles.[3] So when Ministers claim that "the Data Protection Act applies" the claim can be disingenuous,[4] if Ministers can subsequently use powers to modify the impact of the Principles.

(c) Parliament does not receive the information it needs to scrutinise legislation in the field of Human Rights.[5] This problem is especially acute in the field of national security[6] and DNA profiling.[7]

(d) Parliamentary procedures are not responsive to the increasing number of international commitments and treaties which require transfers of personal data from the UK to other countries.[8] The European Parliament has little power in respect of decisions made at the Council of Ministers. Often

1 For example, powers specified in the ID Card Act 2005, Children Act 2004, Anti-Terrorism, Crime and Security Act 2001.

2 HMRC often justify taking copies of databases under the Taxes and Management Act of 1970. Parliament did not discuss this Act in the context of database access—mainly because the technology was not developed (eg in 1970, a mainframe computer with 256K of memory—which filled a large room—was a rarity—now a memory stick measuring a couple of inches has 10 times as much memory). My own view is that Parliamentary approval should somehow be refreshed whenever technical innovation changes the nature of the use of powers.

3 Section 12 of the Children Act 2004, for example, allows Ministers to enact powers which can apply to the content of personal data store on a database as well as accuracy, security, retention, management, disclosure and access.

4 A general statement on the lines that "the database will comply with the Data Protection Act" was given, for example on 20 April 2006: Column 807W; and 20 July 2005 : Column 1784W and 16 November 2004 : Column 1430W in relation to ID Cards Act. Or 1 September 2004 : Column 774W and 2 November 2004: Column 228 for the Children Act 2004.

5 19th Report of the Joint Committee on Human Rights (session 2004–05) calls for a "Human Rights Assessment" to be published.

6 Joint Committee On Human Rights, Third Report ("Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters"), Session 2005–06, Written Evidence 156.

7 See comments made by the Science and Technology Parliamentary Select Committee ("Forensic Science on Trial", session 2004–05), around paragraph 75.

8 International Treaties or Decisions of the Council of Ministers are often presented to Parliament as fait accompli and expanded upon—for example the ICAO agreement to capture two fingerprints was used in Parliament to justify the capture of all 10 fingerprints for the purpose of the ID Card.

decisions are imposed on the UK Parliament on the grounds that the UK has to sign up to an international commitment.[9]

(e) Parliament has not been given any background to the reasons why the European Commission think the UK's Data Protection Act 1998 is deficient; nor has Parliament explored these issues, yet Government often claim that processing of personal data will be protected by the Data Protection Act.[10]

Scrutiny of Secondary Legislation

3. Parliamentary procedures with respect to secondary legislation can lead to problems in the way scrutiny is effected, and this can be illustrated by the letter the Home Secretary wrote to the Joint Committee on Human Rights in relation to the ID Card scheme.[11] The Home Secretary claimed that if the detailed implementation of powers by Statutory Instrument (SI) breached the Human Rights Convention, then these SIs could be struck out by the Courts using its powers under the Human Rights Act. It follows that all human rights issues can be considered by Government when the instrument is drafted and not when the powers are being obtained.

4. There are several problems raised by this approach:

(a) Government can use the "powers could be struck-out" argument to ignore any criticism in Select Committee Reports which relate to wide ranging powers.[12]

(b) scrutiny of primary legislation by Parliament when granting the powers can be limited because of the timetabling procedures can be used by Government to limit debate on important topics.

(c) the secondary legislation associated with the use of powers is not subject to line by line scrutiny or much debate.

(d) Ministers can expect the use of their powers to be approved by Parliament and it is a very rare occurrence that an SI is defeated or withdrawn;[13] there are about 2,500 Statutory Instruments (SI) per year and, unless the SI is technically defective, most are not challenged.

(e) Pre-legislative scrutiny by Parliament is effectively replaced by post-legislative scrutiny by the Courts. If a Court were to strike out a Ministerial order, (eg as happened in the field of terrorism), it would bring with it the prospect of further clashes between the Government and the Courts and thereby risk of politicising the judiciary.

(f) scrutiny becomes the preserve of those rich enough (or poor enough in the case of legal aid) to take human rights cases through the Courts in an attempt to strike out statutory instruments. This legal tussle is also an unequal struggle—the average citizen is pitted against a Government which has access to a bottomless public purse and teams of its own lawyers, if need be.

(g) If secondary legislation were to be struck out by the courts, it is possible to envisage circumstances where Ministers would just draft another alternative instrument circumventing any legal problem. The result could be that any legal challenge would need to start again at square one.[14]

5. The JCHR has already commented on the problems identified above in its 19th Report. This Report recommended that Government should publish, with each Bill, a Human Rights Memorandum[15] which justified how any proposed Bill was compatible with obligations under Human Rights legislation.

[9] The forthcoming third pillar Directive, the data retention arrangements in the field of telecommunications, the European Commission agreement on the transfer of PNR data to the USA (when it comes) all provide examples where scrutiny by the UK Parliament can be limited.

[10] FOI requests dealing with these details have been denied on the grounds that release would jeopardise international relations (Decision Notice FS50110720 on the OIC web-site) and Parliamentary Questions (28 November 2005 : Column 126W; 20 June 2005 : Column 814W) have not provided any meaningful information. The hearsay chatter on the grapevine is that the Commission has unease at the UK's Data Protection Act because: (a) the Court has unfettered discretion to deny the right of access to personal data; (b) the powers of the Commissioner are weak; (c) the transfer arrangements under the 8th Principle are not exactly as the Directive requires; and (d) the definition of personal data is too narrow. The definition of Relevant Filing System is seen to be too narrow, but the Commission recognises that the extent to which manual files are covered is subject to the discretion of Member States when implementing the Directive.

[11] Joint Committee On Human Rights, 8th Report, Session 2004–05, Appendix 1.

[12] See recommendations 59 and 60 of the Home Affairs Select Committee report into ID Cards (session 2004–05) where the powers were described as "unacceptable", yet they exist in the ID Card Act 2006 in the same form.

[13] One SI on a privacy matter which was withdrawn was the draft SI issued by David Blunkett in relation to wide access to Communications Data (as defined under RIPA). Press reports at the time credited Mr Blunkett's son (Hugh) for the Home Secretary's change of mind (see for example, http://news.bbc.co.uk/1/hi/uk_politics/2051117.stm).

[14] This is the practice with respect to National Security Certificates signed under section 28 of the Data Protection Act (eg in the case of Norman Baker MP). Mr Baker won his case, only to be given a further certificate applying the exemption.

[15] Session 2004–05, paragraph 81 states that the Government should: "identify the Convention rights and any other human rights engaged by the bill, and the specific provisions of the bill which engage those rights"; "explain the reasons why it is thought that there is no incompatibility with the right engage; "where the rights engaged are qualified rights, identify clearly the pressing social need which is relied on to justify any interference with those rights"; "assess the likely impact of the measures on the rights engaged"; "explain the reasons why it is considered that any interference with those rights is justified";" cite the evidence that has been taken into account by the Department in the course of its assessment".

6. The Government has not accepted the above recommendation.[16] It is difficult to see how Parliament can scrutinise effectively without the above information, and I suspect that many members of the public would be surprised to lean that Parliament does not have access to such information.

Why Privacy is at Risk?

7. The Data Protection Act does not protect privacy to the extent imagined. I have detailed these arguments elsewhere[17] but I summarise the main points below.

(a) Data sharing policies have the effect of merging Government Departments that share personal data into a single data controller, whereas the Data Protection Act assumes an array of separate data controllers. This change arises because data sharing statutory gateways allow personal data collected for one purpose by one Department to be used for other purposes under the control of different Departments. In data protection terms, this especially degrades the protection afforded by the Second Principle (purpose limitation).

(b) Legislation often defines widely drawn purposes (eg the purpose of "the efficient and effective delivery of public services" as defined in the ID Card Act). This degrades the protection of those Principles which are usually interpreted assuming a narrowly drawn "purpose" of the processing.[18]

(c) Retention policies (eg DNA database, communications data, retention of ID Card data) enhance the surveillance potential of the data and raise questions of trust.[19] If Government is delivering joined-up services, the risk is that mistrust of one part of Government activities is likely to also become joined-up and extend to all Government services.

(d) Government Ministers are often responsible for policies which require interference with private and family life, or have oversight or responsible for the organisations which undertake such interference. A conflict of interest arises as these Ministers, at the same time as being accountable for this interference, establish the procedures which protect private life from such interference.

(e) Whereas government services are becoming joined-up, the protection afforded by the regulators who operate in the area of law enforcement and national security are becoming increasingly disjointed.[20]

(f) The Information Commissioner, when he raises privacy issues which need to be resolved, is seen by Government (and is often treated as such) as part of the opposition to the policy. The result is that privacy concerns form part of the political debate about the policy (ie whether personal data should be processed) and often are not fully addressed in the implementation of policy (ie how to process personal data).[21]

(g) The Information Commissioner is not a powerful regulator. The Commissioner cannot audit compliance with the Data Protection Act without permission; the Commissioner cannot "name and shame" transgressors following an assessment without permission; the Commissioner cannot fine data controllers that breach a data protection principle.[22]

(h) Data retention policies are likely to be subject to function creep. The reason is that retained data are stored on a systems that costs £millions and there will be pressure to demonstrate value for money

[16] I was told by the Clerk to the JCHR when I was preparing this paper that "The Government has not agreed to this recommendation (in the 19th Report) and is not providing Human Rights Memoranda in relation to Bills. From the start of this Session it has been making an effort to meet the spirit of the Committee's recommendation by improving the quality of treatment of human rights in the Explanatory Notes which accompany each Bill. The Committee has not yet taken a view as to whether it considers these efforts meet its requirements".

[17] Details in Home Affairs Committee, 4th Report, "Identity Cards", Session 2003–04, Volume II (Ev 169–73 & Ev 276–81).

[18] For example, if someone says "data item X is relevant to a housing benefit purpose", the claim can objectively be tested- is the data item relevant or not relevant to the housing benefit purpose? However, this kind of test is substantially diminished if the purpose is broadly defined. In the ID Card Act, for example, one purpose relates to "the efficient delivery of public services" which means that to show a breach, the Commissioner has to establish "inefficiency". Most of the data protection principles are defined in terms of a purpose which is assumed to be narrow; the broader the purpose, the narrower the protection afforded by the Principle.

[19] There are examples of trust being lost. For example, parents who object to the police retaining DNA of their children who have been mistakenly arrested, parents who object to their children's details being retained on a child at risk register when there is no risk, and patients who object to the holding of limited medical details centrally on the NHS spine.

[20] Oversight of the Intelligence Services (except interception practices) is carried out by the Intelligence Services Commissioner. Oversight of interception is carried out by the Interception of Communications Commissioner. The Office of Surveillance Commissioners is responsible for oversight of property interference under Part III of the Police Act, as well as surveillance and the use of Covert Human Intelligence Sources by all organisations bound by the Regulation of Investigatory Powers Act (RIPA) (except the Intelligence Services). There is an Information Commissioner, a National Identity Scheme Commissioner, the Commissioners who deal with Northern Ireland policing/terrorism and the Police Complaints mechanisms and the various Parliamentary Ombudsman could also be drawn into the supervision business. Recently the Financial Services Authority levied a £1 million fine in a case of inadequate security of personal data held by the Nationwide Building Society.

[21] The Information Commissioner's views on the ID Card provides an example. The Home Secretary said that the Information Commissioner was "a long-standing opponent of the identity card system" (28 June 2005: Column 1157).

[22] Unlike the FSA which recently fined the Nationwide £1 million for breaches of security of personal data.

(eg by using the data for other purposes). That is why the NIR started life as a security system and is now a public administration, identity management and security system.

(i) Data retention policies require the public to trust the authorities performing the interference. The public has to trust that any use of retained data is limited to justified purposes approved by Parliament. The public have to trust that all staff who have access to the data are fully trained not bend the rules. The public has to trust that procedures which authorise interference are followed scrupulously. The public have to trust the politicians not change the law or use powers to permit function creep. All this trusting is one directional—from the public.

(j) The merger of security and privacy on the European Commission model is not the solution as this risks making privacy subservient to the security objectives.

Overcoming a Structural Problem

8. I think a major problem lies the fact that the public body or Minister responsible for policies/procedures that require interference with private and family life can also establish the policies/procedures which protect the public from over-zealous interference. The Home Secretary, for instance, produces Codes of Practice with respect to interference and safeguards in relation to policing, data retention, surveillance, immigration and national security matters. A recent example is the Serious Crime Bill where the Audit Commission are given powers to extend its data matching responsibilities (ie interference) and produce a Code of Practice which offers protection. As a matter of general principle the responsibility to interfere should be separated[23] or distanced from the responsibility to identify safeguards. As will be seen, such a separation could give Parliament an active role in determining public policy with respect to privacy versus security.

9. For example, suppose a Minister had to draft a Code of Practice for the processing of personal data in circumstances where the Commissioner had to approve the Code of Practice before the processing could commence. This means that the Commissioner would be able to withhold approval on grounds, for example, that the Code breached a Data Protection Principle or would be in breach of Article 8 of the Human Rights Act. You could have procedures where the Commissioner's view of the law could be tested, as of now, via a Tribunal system which could lead, via an appeals process, to the Courts.

10. Obviously, if there were to be a disagreement over a Code of Practice, there would be a period of negotiation where by the Secretary of State and Commissioner would try to agree. If such negotiated agreement occurred, then all well and good—the Code of Practice comes into operation. If no agreement was possible, the Secretary of State could ultimately override the Commissioner's objections by exercising powers that need an affirmative resolution before the provisions of a contested Code of Practice could come into effect.

11. The affirmative resolution requirement would mean that any disagreement would be brought before Parliament for a decision on the use of powers by a Minister, and before Parliament makes the decision, it can be fully informed as to the nature of the problem (eg take evidence from the Commissioner and Minister etc). However, at the end of the day, it is Parliament that is defining, publicly, where the balance between interference and privacy should arise—and not the body/Minister who is responsible for the interference.

12. There is also a need for a mechanism to allow a Code of Practice to be changed by the Commissioner after it has come into effect (eg where changes are needed because the practical effect of the Code has become apparent). There again, in the case of unresolved disagreement, powers, needing affirmative resolution of both Houses of Parliament could be made available to the Secretary of State. If the powers are used so that the SoS comes to Parliament for a decision. Again, it is Parliament having a role in defining the boundaries of social policy with respect to security versus privacy—rather the Secretary of State taking these decisions in isolation.

13. However, as soon as you have a mechanism which allows the Commissioner to change Codes of Practice, then it is easy to graft on a mechanism that allows data subjects/data controllers to press for changes to a Code of Practice. For example, data subjects can argue for a change in the Code of Practice because it is defective, whereas data controllers can argue for changes which reflect new processing circumstances. This kind of mechanism directly engages both groups of stakeholders in a data protection Code which effects them – namely, data subjects and data controllers. Codes of Practice become dynamic and responsive.

[23] I have developed a mechanism whereby Codes of Practice can be challenged by stakeholders—this can be made available to the Committee if it wants it. However, the fundamental point is a separation of powers—if the Minister has power over interference, he does not have the main levers of control over the degree of protection on offer.

Constitutional Issues Arising from a Lack of Scrutiny

14. The Appendix to this evidence illuminates a final constitutional issue; it arises when, for whatever reason, Government does not want something to be scrutinised. The "something" in this case relates to the Identity Card Scheme and the decision to use the National Identity Register (NIR) as a population register (the NIR is the database associated with the Scheme). The way that this decision was reached, in my view, raises questions as to whether Parliament is in a position to scrutinise any legislation effectively.

15. For instance, is it "constitutional" for the Government to use of the NIR as a population register:

(a) when the two public consultations on the ID Card specifically excluded the use of the NIR for this general public administration purpose.[24]

(b) when the Government promised a further public consultation as it was necessary "to explore the issues around public acceptability of the proposal"[25] (to establish a population register).

(c) when the Government's responses to several Parliamentary Committees (eg to the Home Affairs Select Committee in October 2004) and to Parliament do not fully reflect the decisions that had been taken.[26]

16. In general, officials (and one assumes Ministers) knew before the General Election of 2005, that the intention was to use the NIR for a general public administration purpose. This fact could have featured as part of the General Election debate (and could have received an electoral mandate for this part of the ID Card program). As it was known that the use of the NIR for a general public administration purpose represented 20% of the business case for the ID Card scheme, should this fact have appeared in the ID Card Bill's Regulatory Impact Assessment laid before Parliament? Should a Ministerial statement informing Parliament of the change of use of the ID Card scheme been delayed for nine months until after Parliamentary scrutiny of the ID Card Bill was complete?[27] Should one of the several Parliamentary opportunities presented to Ministers to announce important changes to the ID Card scheme been taken?[28]

17. If the politics of accountability, scrutiny and debate over public policy cannot be channelled through a Parliamentary process on a subject as mundane as "efficient public administration", how can Parliament assume it has properly scrutinised any other governmental policy? Given that the next Prime Minister has already signalled his intention to grant Parliament more powers of scrutiny, my hope is that the evidence presented in the Appendix plays a part in these new constitutional arrangements.

18. For convenience, I have added to the Appendix, commentary which relates to the Committee's two Reports into the ID Card Bill on 17 March 2005 and 12 October 2005.[29] My own view is that if the Constitution Committee had been aware that the decision had been taken to use the NIR as a general public-sector information resource then I suspect these Reports might have been worded differently.

19. Finally, there is wide-spread concern that Parliament is no longer the focus of political and policy debate. Perhaps the evidence in the Appendix goes a long way to illustrate one reason why this is the case.

May 2007

[24] The public consultations (CM 5557&CM 6178) both gave commitments to use the ID Card and related NIR for limit purposes (eg to crime and security issue).

[25] Paragraph 3.20 of CM 6178 ("Legislation on Identity Cards").

[26] The Appendix identifies several Parliamentary opportunities presented to Ministers to announce the change of use of the NIR to support a public administration purpose; these were not taken. The several statements made by Ministers to Parliament about the use of personal data held in the NIR are very difficult to reconcile with the statements made in minutes of meetings with civil servants made months earlier than the Ministerial statements.

[27] See Appendix 1 and the events of 30 June and 13 July 2005.

[28] A sample of these are referenced in the text in the Appendix. However, around the time of the First Reading of the ID Card Bill in June 2005, and to avoid accusations of "function creep", civil servants advised that a statement should be made to Parliament concerning the NIR's wider role in general public administration. A Ministerial Written Statement was prepared but its publication was delayed until three weeks after the ID Card Act 2006 had passed through Parliament.

[29] Select Committee on the Constitution (5th Report, Session 2004–05, HL 82; 3rd Report, Session 2005–06, HL 44) both on the ID Cards Bill.

APPENDIX 1

"APPENDIX: TIMELINE OF THE DECISION TO USE THE NIR AS A POPULATION REGISTER

INTRODUCTION

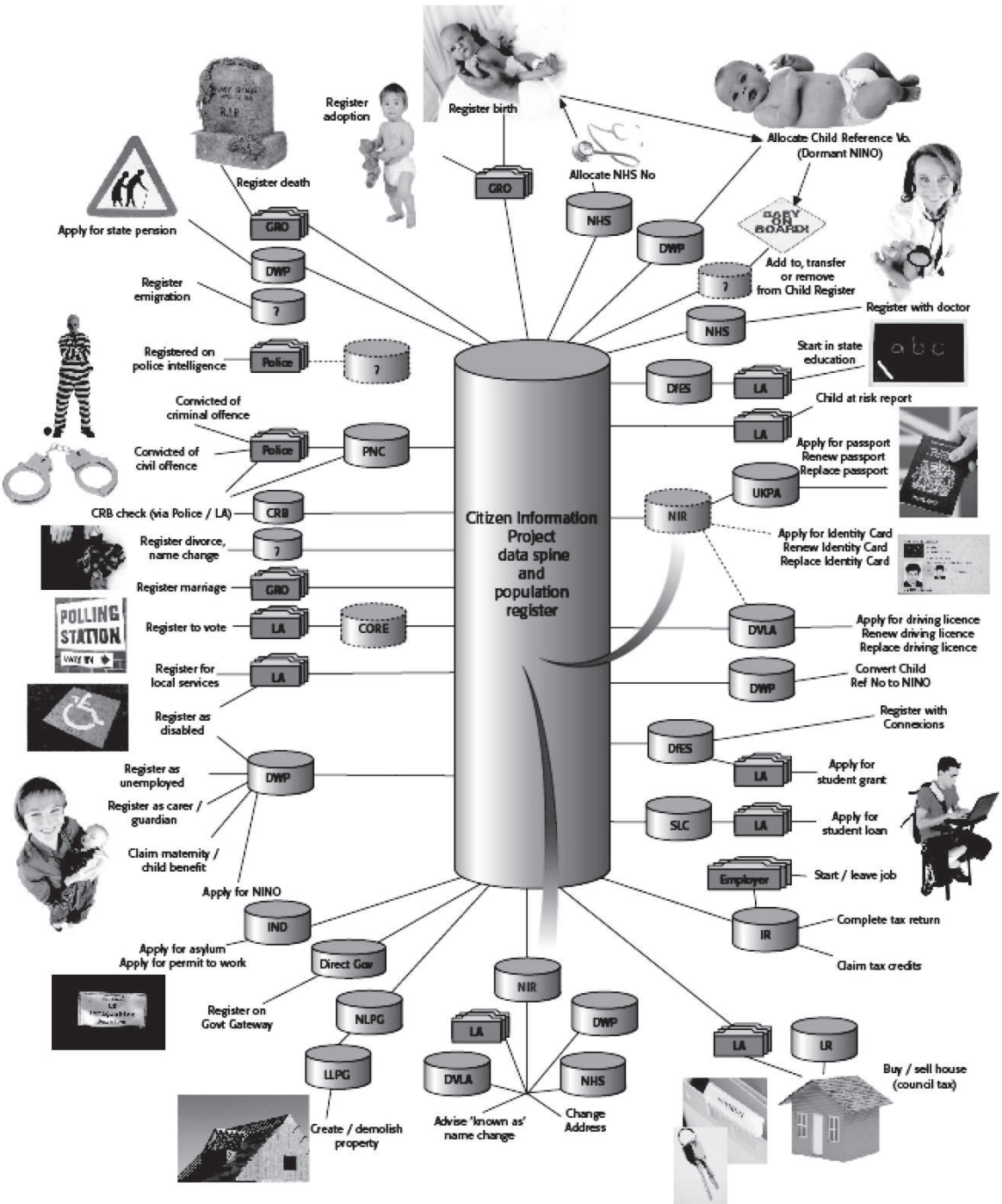
A1. When I gave oral evidence before the Home Affairs Select Committee in its inquiry into the draft ID Card Bill, I made the remark that a comprehensive public administration function should not be "piggy-backed" onto the National Identity Register (NIR), the name for the database associated with the ID Card system, without a thorough public debate as to the consequences.[30] The evidence I now lay before the Committee (in this Appendix) concerns how these plans were made without effective scrutiny by Parliament and contrary to a promise of a further round of public consultation.

A2. For example, months before Constitution Committee's Reports into the ID Card Bill (eg in September 2004), the Home Secretary knew that the ID Card had to be compulsory to realise the public service efficiency savings if the NIR was also to serve as a population register (the diagram on the next page[31] was produced by officials in July 2004). I am sure that if the Committee, concerned as it was about the relationship between the state and individual, was aware of this development, then it would have featured in the text of its reports. I am also confident that the Committee would have expected Ministers to refer to this development in their submissions to the Committee. However, for some reason the Committee (and Parliament) was not informed of this incorporation until the ID Card Act had been passed into law—even though this incorporation had been established as Government policy before the ID Card Bill had been printed in July 2005.

[30] Q782, Fourth Report of Home Affairs Committee, Identity Cards, Session 2003-04, Volume II.
[31] From *CIPPB(04)22* (produced July 2004) and in "*Engineering and Technology*" (November 2006).

Your digital footprint, from cradle to grave

This diagram, based on one produced as planning for a Citizen Information Project, shows how many government agencies hold data on us. It also illustrates the concept of data creep: when the original was drawn, the Citizen Information Project and the National ID Register were separate functions (as shown). The two projects were merged as part of the 2006 ID Cards Act, although this wasn't disclosed to Parliament until afterwards.



A population register

A3. The essential idea behind a population register is that all public authorities should be able to exchange (ie update and download) basic personal details via a central repository. By doing so, the system creates connections between diverse databases involved in such exchanges. There are obvious efficiency savings to be made when such data sharing is undertaken (eg the population register negates the need for a national census). However the risks are also apparent if the population register is associated with an audit trail which possesses an ability to enhance the link between public sector sources of information associated with each citizen (eg tax, social security, health, police, education)[32] and which is intended to extend to private sector information (eg opening a bank account, hire of a car).

A4. The decision to widen the use of the NIR to include a population register fundamentally changes the surveillance role of the NIR. No longer is the purpose of the NIR limited to law enforcement and security where a reason to interfere with private and family life can be justified in terms of security, crime or immigration. Because of section 1(4) of the ID Card Act 2006 refers to "the purpose of securing the efficient and effective provision of public services", the efficiency of rubbish or council tax collection could become a legitimate reason for interference.

A5. The security implications are also different—basic details from the NIR are potentially accessible to hundreds of thousands of public servants in any public authority. The civil penalty of not to keep the address details on the NIR could be viewed as a civil penalty not to update any public authority record (eg such authorities could report those who fail to update address records on the NIR). Who should run such a system also becomes an issue for legitimate debate—should it be the Home Office with its emphasis on security and crime, or the Office of National Statistics (ONS) which has a public administration ethos and is trusted by the public with respect to the Census? It is important to note that all these questions (and others) raise valid subjects of concern which could have (and should have) been debated when the ID Card Bill was before Parliament and that the ONS had identified about thirty issues of this nature.[33]

A6. The basis of this analysis in this Appendix has been published in *Data Protection and Privacy Practice (July 2006)* and provided to the Committee in a form which it has been updated and fully cross referenced. That updating has unearthed further information which has not been published.

2002 and 2004—The public consultations deny wide use of ID Card database

A7. The Consultation Document launched by David Blunkett in April 2002 posed an interesting question: "As an entitlement card would need to be underpinned by a database of all UK residents, an issue for consideration is whether this database should be a national population register . . . or a new self standing database".[34]

A8. The answer came in the subsequent document "Legislation on Identity Cards" (CM 6178) published in April 2004. Under a Chapter entitled "Wider issues **not** included in the draft legislation" (my emphasis), it stated that "The National Identity Register and a population register are separate but complementary proposals and they serve different purposes" but the Government was "open to the possibility of including provisions relating to the creation and operation of a separate population register within the identity cards legislation" (Paragraph 3.21).

A9. Paragraph 3.20 of CM 6178 also promised that further legislation would be needed to establish a population register; it stated that further work would be undertaken and, that further developments "will also include public consultation to explore the issues around public acceptability of the proposal" so that any new "legislation would also introduce concrete safeguards for the public".

A10. In summary, the public was informed that the NIR was to support security matters—there were overlaps with a population register but they were separate databases requiring separate legislation, and that access to the NIR by law enforcement agencies would be strictly limited.[35] In relation to a population register, a further public consultation was promised "to explore the issues around public acceptability of the proposal".[36]

[32] See Sections 1(5)(i) and 3(4) of the Identity Cards Act 2006 which shows that any reference to an entry in the NIR will leave such a footprint in the audit trail.

[33] CIPPB(04)(02) "Citizen Information Project: project definition stage—aims and policy issues" dated February 2004 on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp.

[34] "Entitlement Cards and Identity Fraud", Cm 5557, paragraph 2.40.

[35] For example paragraph 3.29 of CM 5557 states that "the Government would want to see a full debate on this point and seek views on what safeguards there should be. For example, whether access to the database in these circumstances should be governed by a warrant applied for on a case-by-case basis". The question posed of the public was whether law enforcement agencies should have access to the central register "in closely prescribed circumstances" such as "national security or very serious crimes".

[36] Paragraph 3.20 of CM 6178 ("Legislation on Identity Cards").

April 2003—Legal advice and the CIP

A11. Between the two public consultations, and prior to commencement of the Citizen Information Project (CIP), legal advice was taken ("Final Report, Annex 8: Legal issues").[37] This advice stated that if the population register contained limited contact details and if data sharing of these details were to be legitimised by legislation, then such legislation was unlikely to breach Article 8 of the Human Rights Act. The advice judged that any "interference by a public authority" in terms of Article 8(2) would very likely fall within a state's "margin of appreciation". This conclusion effectively told Government that it could lawfully draft data sharing powers, which permitted basic contact details about individuals to be shared across the public sector, without consent of the citizen. The data protection elements related to the First and Second Principles would also be resolved, as these cover essentially the same ground as Article 8.

A12. The general benefits of the CIP database were listed in this legal advice. These were described as: "ensuring that public bodies have accurate information about citizens"; "financial savings to the public purse"; "a reduction of the potential for fraud"; "speedier location of citizen records"; "reduced occasions when one citizen is confused with another"; "reduced occasions when communications between the state and citizen are sent to out-of-date addresses"; "simplified arrangements for citizens to notify changes of name and address"; and "improved targeting of public services and formulation of government policy".

A13. The data items listed in the advice were: "names including name history"; "addresses including multiple addresses and address history"; "sex"; "place of birth"; "date of birth" and "unique identifier number". The advice did not consider that the NIR would become the database for the CIP.

A14. This legal advice was obtained before the first meeting of CIP in February 2004 (CIP meetings involved staff from many Government Departments and senior personnel from the ID Card project were always in attendance). The advice contained sufficient detail to stimulate a public debate on the CIP if the Government wanted such a debate.

April 2004—Draft ID Card Bill published

A15. Clause 1 of the draft ID Card Bill[38] identified one expansive statutory purpose which enabled information recorded in the National Identity Register (NIR) "to be disclosed to persons in cases authorised by or under this Act". Clause 23 of that draft Bill identified a power which allowed the Secretary to State to authorise disclosures from the NIR, without consent, for prescribed purposes which were unconnected with terrorism, national security, crime, taxation, and immigration.

A16. It is clear that these two provisions were drafted in a sufficiently broad way to provide the legal framework for the use and disclosure of NIR data for the public administration purposes which was consistent with the CIP's legal advice obtained in April 2003. So if the intention was for the NIR, established by ID Card legislation, to assume CIP functionality, the Government was clearly in a position to inform the public and Parliament of this step. For example, during the first half of 2004, the Home Affairs Select Committee of the House of Commons was studying the Government's ID Card proposal in detail.

A17. It can be argued that at the text of the draft Bill studied by the Committee reflected the fact that the CIP and NIR were seen as separate. In the draft Bill, the general public sector purposes were "to ensure free public services are only used by those entitled to them" and "to enable easier and more convenient access to public service". These purposes are more limited than the broadly defined "the efficient and effective delivery of public services" purpose found in Section 1(4)(e) of the Identity Cards Act 2006.

March to June 2004—CIP is separate from NIR

A18. There is further evidence which suggests the two schemes were originally seen as separate. For example, the CIP Project Definition[39] prepared for CIP meetings in Spring 2004 identified around 30 policy issues to resolve. These included "Who should run the live register?" and "establishing trust in the organisation running the population register". Another document prepared for the CIP Project Board stated that a stand-alone Population Register Bill was the preferred option.[40]

[37] Annex 8 is on http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp.
[38] Published in April 2004 in CM 6178.
[39] CIPPB(04)(02) "Citizen Information Project: project definition stage—aims and policy issues" dated February 2004 on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp.
[40] CIPP(04)12—"Towards a Legal Strategy" on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp.

A19. Other evidence also supports the view that the CIP and NIR were seen as separate:

— **29 March 2004**[41] MPs were told "The CIP, the National Identity Register (part of the Government's proposals for an identity card scheme) and the NHS data spine are separate but complementary projects". Although the answer indicated that there could be integration "in the future" the key information given to Parliament was they were currently independent.

— **20 May 2004**[42] The CIP minutes of that date recorded a general agreement that a discussion paper According to these minutes, document CIPPB(04)19 provided "a clearer view of the distinction between CIP and IDC" (IDC = Identity Card).

— **18 June 2004**[43] The CIP minutes of this date recorded a Home Office official involved in the ID Card project stating that he thought "the overlap between CIP and NIR more apparent than real" because "CIP functionality does not overlap with the identity card core proposition" (eg the NIR is not designed for "pushing change of contact details out to the public sector" or "holding multiple addresses to support joined up Government"). The minutes also reported that "Project Board members preferred the stand-alone option for CIP" and that the Home Office were worried about "scope creep weighing down the identity cards programme".

— **June 2004** A second round of public consultation reassured the public that "The register will not be open for general access" (CM 6178; "Legislation on ID Cards", paragraph 2.6) and that "The National Identity Register and a population register are separate but complementary proposals and they serve different purposes" (paragraph 3.21). The diagram following footnote 2 of this submission shows the extent of CIP functionality.

Using the NIR as a population register was always a possibility—March 2004

A20. A document made available to CIP personnel in March 2004[44] made it clear that "The Home Office has indicated that they are not averse to including CIP clauses" in an ID Card Bill because it had "already a slot in the legislative timetable". However, there were risks of "the Population Register being closely identified with the ID Card scheme" and that separate legislation would make it easier "to prohibit police or security access to the Register". Separate legislation would also "limit scope-creep" and would "set the Population Register clearly apart from ID Cards and allow it to be seen as a benign tool for improving public service". However, the "Home Office might consider that (separate) CIP legislation, if contentious, put the ID Cards scheme at risk".

A21. It concluded the decision to use the NIR for a population register "may become the preferred option if the Minister makes a decision about CIP in time for CIP powers to be included in the ID Cards Bill".

10 and 16 September 2004—CIP's population register should be part of NIR

A22. By the end of the summer these dilemmas had been resolved in favour of using the NIR as a population register for general public administration purposes. A letter dated 10 September 2004[45] was sent from the CIP project board to the Chief Secretary of the Treasury which stated that the merging of CIP into the NIR would "strengthen the VFM case for ID Cards". It therefore recommended that "the Home Secretary[46] be asked to include improving the efficiency and effectiveness of public services as a purpose of the Identity Card" and that "the NIR should become the national adult population register long term (but only if ID Cards become compulsory)".

A23. The letter also explained that the broad concept of a CIP had gained acceptance with the focus groups but when the detail of the CIP project were explored by these groups "concerns are raised that whether the potential benefits could justify the cost and that this would lead to linkage of sensitive personal information across government".

A24. The CIP minutes of 16 September 2004 supported the integration of the NIR and the CIP. These stated that the "ID Card legislation presents no impediments to the NIR sharing data with other registers to support their statutory purpose" and it was recognised that "the CIP position is now reflected within the ID Card Bill".

[41] Answer to PQ 163155, 29 March 2004.
[42] From http://www.gro.gov.uk/cip/Definition/ProjectBoardMinutes/index.asp.
[43] From http://www.gro.gov.uk/cip/Definition/ProjectBoardMinutes/index.asp (Minutes confusingly posted under the date of 21 July).
[44] CIPP(04)12—"Towards a Legal Strategy" on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp.
[45] Citizen Information Project: CIP progress report—10 September 2004 on http://www.gro.gov.uk/cip/Definition/ProjectBoard Papers/index.asp.
[46] David Blunkett MP was Home Secretary till mid-December 2004, then from that date, Charles Clarke MP.

The minutes also show that the Home Secretary would know of the change: it stated "Home Secretary to write to cabinet colleagues in early October to clear some changes to the IDC Bill. This will include greater clarity on the statutory purposes of the scheme, including the purpose of supporting greater public sector efficiency".

24 September 2004—Privacy Impact Assessment completed

A25. A preliminary Privacy Impact Assessment (PIA) for the CIP was finalised in September 2004 (published in "Final Report, Annex 8: Legal issues")[47] and succinctly identified the benefits of the CIP project as they were known at this date. Because of the merger of the CIP into the NIR, these benefits also applied to the ID Card scheme. The Assessment split the benefits of the CIP into three groups:

- **Benefits to the individual**: "only have to notify one government department of a change of address" and "once the citizen has changed contact details to one department, their responsibility to notify other departments is relinquished"; an up to date register will "allow citizens to receive personalised and targeted communications"; and improved services "as it is easier for the service provider to find the files".
- **Benefits to the tax payer and society**: "contact details up to date"; facilitate "internet services"; cost savings through better "tracing individuals", "reducing fraud"; "ensures every individual fulfils their obligations to the community" (whatever this means!); improvements in data sharing.
- **Benefits to government**: keeping contact details up to date; less waste of resources when tracing individuals; snapshots of population movements; targeted mailshots to citizens; better statistical analysis; provides a biographical footprint (because there is a record of those public bodies which use the address in delivering services to the individual); and savings as appointments always have up-to-date details.

A26. Given the Home Affair Select Committee's interest in the concept of a Privacy Impact Assessment, it is noted that the senior civil servant from the ID Card project is recorded in the minutes[48] as expressing interest in the PIA for the CIP's population register.

End of September 2004—a status summary

A27. By the end of September, in relation to the use of the NIR for "the purpose of securing the efficient and effective delivery of public services", the evidence suggested:

- the CIP and NIR were intended to be fully integrated and CIP functionality was to be implemented by the powers Ministers were seeking under the ID Card Bill which was before Parliament;
- Ministers decided to use the ID Cards Bill to implement the integration of CIP and NIR;[49]
- that consent of the individual would not be needed to permit data sharing to achieve CIP benefits (legal advice; April 2003);
- both public consultations on the ID Card had reassured the public that there would not be general access to NIR and that there would be another round of consultation about a population register;
- the purposes associated with the CIP which were to be integrated into the NIR were well defined and detailed; and
- in order to merge the CIP with the NIR, **the ID Card had to be compulsory and Ministers knew this.** (Note: this emphasis is given because I have been unable to find **any** Ministerial statement which explained the need for a compulsory ID Card in terms of implementing CIP functionality).

October 2004—Government replies to the Home Affairs Committee ID Card Report

A28. However, in its official response, MPs on the Home Affairs Committee were told that the Government) was "no longer actively exploring plans to develop a separate population register but rather will be exploring options to improve the quality and effectiveness of existing registers".[50] As the NIR is **not** an **existing** register, this statement cannot refer the NIR which had not yet been created.

A29. The Government also told the Committee in its official response that it believed that "the NIR has the longer term potential to fulfil some of the functions envisaged for the national population register". This statement with its reference to "potential" is difficult to reconcile with the definite position as recorded in the

[47] Annex 8 is on http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp.
[48] The minutes of 25 November 2005.
[49] see CIPPB(04)12—reference 53.
[50] Paragraph 44 of CM 6359.

minutes taken a month earlier (16 September 2004) which stated that "ID Card legislation presents no impediments to the NIR sharing data with other registers to support their statutory purpose" and that "the CIP position is now reflected within the ID Card Bill".

A30. The Government's reply did not go into detail as to the nature of these "longer term" functions, even though these were set out in the legal advice of April 2003 and in the Privacy Impact Assessment of September 2004. Nor did the Government reveal that the legal advice stated that consent of ID card-holders was not needed to permit sharing of contact details to achieve CIP functionality. Also absent in the Government's reply was any explanation that powers in the proposed ID Card legislation were broad enough to legitimise data sharing of a general administration purpose.

A31. It is interesting to note that Recommendation 38 of the Committee's Report had stated that "The Government must be clear and open about the issues involved and enable informed parliamentary and public scrutiny of any decisions". The Government's response to this recommendation was unequivocal: "The Government agrees this is an important issue".

28 October 2004 (Col 53WS—First written statement about the CIP)

A32. The Government informed Parliament of a "feasibility study" which found that a "UK population register has the potential to generate efficiency benefits" and that "if ID Cards were to become compulsory, it may be more cost effective to deliver these benefits (efficiency savings) through the NIR". The statement also does not reflect the status of the project as described in September 2004 (eg "the CIP position is now reflected within the ID Card Bill") and is very low key. Its use of words such as "feasibility", "potential", "if" and "may" makes the statement less definite than the decisions which **had** been taken.

A33. There was a promise of a further statement after June 2005 when a "second stage of project definition" was completed. This also reinforces the idea that matters have not yet been determined.

29 November 2004—Regulatory Impact Assessment published

A34. Home Office Minister, Des Browne MP, signed a Regulatory Impact Assessment (RIA) which was produced to provide Parliament with details which related to the impact of the ID Card Bill. The section of the RIA dealing with "more efficient and effective delivery of public services"[51] described the use of the ID Card to achieve savings. It did not refer to the fact that far more efficiency savings were to be realised by sharing the personal data in the NIR. The RIA did not reflect the CIP minutes of 16 September 2004 which noted that "the CIP position is now reflected within the ID Card Bill". The RIA did not even illustrate the range of benefits to individuals, government and society which were specified in the Privacy Impact Assessment (dated September 2004) or identified in the legal advice (April 2003).

A35. Similarly, paragraph 26 of the RIA (dealing with longer term benefits) did not mention the decision to use of the NIR for public administration as described in earlier CIP minutes. It tentatively suggested that the National Identity Registration Number "should the card scheme become compulsory" could "provide the means to make more fundamental improvements in the delivery of Government services" but that this step was "not part of the immediate business justification of the scheme". In addition, "the ID Cards scheme could provide a basis for people to notify changes of personal details such as address, only once", but this is "not currently costed as part of the functions of the Identity Cards scheme". (Note: In the letter dated 10 September 2004, the Home Secretary was told that the merging of CIP into the NIR would "strengthen the VFM case for ID Cards"; if one assumes that this statement is based on factual analysis, it is difficult to imagine that some cost estimates did not exist).

9 March 2005—Publication of Constitution Committee's First Report

A36. The Report makes no reference to the public administration purpose and this is presumably because Committee Members were unaware of the decisions that had been taken. However, one passage of the Report lays emphasis on the role of the ONS and the Census Act. It is possible that since the ONS were responsible for the idea of a population register, that the Committee would have strengthened the argument for an independent registrar (modelled on the Census arrangements)—and that the NIR should not be under the control of the Secretary of State.

[51] Paragraphs 64–72 of the Assessment.

18 March to April 2005—CIP benefits form fifth of ID Card business case

A37. The CIP minutes of 18 March 2005 identified "substantial CIP related benefits (address sharing benefits) within HO ID Cards outline business case, amounting to around one fifth of the total". Progress had been such that there was to be a "phased reduction of the CIP team". The Home Office representative stated that she "was able to re-assure the board that there were no anticipated issues with the Identity Cards Bill or the efficiency and effectiveness clause that is relevant to CIP".

A38. In addition, the CIP role was being augmented by the e-government agenda. The representative from the Treasury stated "Working with the Identity Cards programme to establish how Identity Cards could be used to help meet e-government needs" for example "Scoping the issues of e-authentication with service owners and Chief Executives" and "Development of a strategic approach to identity in government including a review of business processes and provision of a risk management framework for e-service delivery in a business sense". The Crosby Review (expected in the summer) could further widen the use of the NIR.

A39. The decision to have wider use of the NIR was in time to have been captured by Labour's manifesto for the 2005 General Election—especially as 20% of the ID Card's business case was being justified on CIP's functionality. Labour's Manifesto itself stated that ID Cards would be established to assist the authorities in purposes connected with crime, terrorism, illegal employment and immigration. There was no mention of the public administration purpose or data sharing of contact details based on the NIR, or that registration on the NIR had to be compulsory (with the implication that the ID Card had to be compulsory) to achieve 20% of the benefits of the ID Card scheme.

A40. The CIP minutes of 15 April 2005 stated that "up to 30 tactical data sharing opportunities (for the NIR) have been identified". These 30 data sharing opportunities have not yet been made public (unlike the 17 benefits which were identified in September 2004 but only made public in April 2006).

25 May 2005—Updated Regulatory Impact Assessment published

A41. After the General Election, on 25 May, the ID Card Bill was re-introduced into Parliament; the Bill specified the "the purpose of securing the efficient and effective provision of public services" and provided wide ranging disclosure powers (in line with the legal advice of April 2003). Home Office Minister (Andy McNulty MP) signed an "updated version" of the Bill's Regulatory Impact Assessment (RIA) to inform subsequent Parliamentary debate on the Bill.

A42. The section on "more efficient and effective delivery of public services" was almost identical with the RIA published 29 November 2004. Although the RIA was promoted as "an updated version" it still did not reflect the use of the NIR to achieve the functionality described in the CIP minutes and background papers (eg minutes of 24 September 2004) and the "30 tactical data sharing opportunities" which had been identified in April 2005 were not mentioned in the RIA. It is also curious that an RIA, which contains many figures which relate to the ID Card, did not state that 20% of the ID Card's business case depended on the merger of CIP into the NIR, or that compulsory entry of contact personal data into the NIR would be needed to implement CIP functionality.

24 June 2005—Final meeting of the CIP project—evidence from the minutes

A43. The final CIP minutes of 24 June 2005 showed that contact details from the NIR would be widely shared (upload and download) and that the Home Office had assumed responsibility for implementing CIP functionality. The minutes stated that the Home Office would have:

- "the responsibility for delivering an adult population register that enables basic contact data held on NIR to be downloaded to other public sector stakeholders" (The "Treasury and Cabinet Office should ensure that NIR delivers CIP functionality as planned");
- "the responsibility for ensuring from around 2021 basic contact data held by stakeholders can be uploaded to the NIR"; and
- to "design the take-up profile of the NIR to be such that population statistics can be realised for the 2021 census".

A44. The CIP's final report which was prepared at this time (but not published until the ID Card Act 2006 had received Royal Assent) stated that secondary legislation (which is in the ID Card Bill) will allow "public services to be provided with NIR data without the need to obtain specific citizen consent".[52] The CIP final

[52] Page 17 of the Final Report.

report also provided examples of how NIR data could be used (which presumably are a sub-set of the "30 tactical data sharing opportunities" identified on 15 April 2005).

A45. The opportunities identified in the Report included:

- "DWP targeting the 300,000 eligible citizens not currently claiming pensions";
- Taxation authorities "contacting employees required to complete self assessment";
- Managing passport application peaks by getting customers to apply early;
- "DfES tracing children at risk via their guardians' addresses;
- "Local councils collecting debt from citizens who have moved to another authority";
- "NHS targeting specific citizen groups for screening campaigns"; and
- "reducing the overall administrative burden on bereaved people".

A46. As the ID Card Bill was commencing its Committee stage in Parliament, there was no barrier to allowing debate to include the new responsibilities of the Home Office as described above.

A47. On 13 June 2005, the Parliamentary Research Department of the House of Commons Library published its 58 page research document into the ID Card Bill. These research documents were produced to inform MPs impartially about the issues—as with the RIA, this research document into ID Cards did not contain details of the decision to merge the CIP into NIR functionality as described above.

30 June 2005—CIP staff wants Parliament to be informed

A48. A draft list of recommendations were prepared by civil servants for the CIP Project Board ("Submission to Ministers—draft")[53] to consider to send to ministers; the list showed that CIP officials were very aware of the privacy and constitutional issues.

A49. Paragraph 2 of the draft recommendations began: "Urgent—Home Office believe there would be advantages in making an announcement before Parliament rises on 21 July so that the Government's intention to use the ID Cards register in this way is confirmed while the ID Cards Bill is still being debated". The reason for this is explained in paragraph 17: "Home Office believe there would be advantages in making an announcement before Parliament rises on 21 July" as "that would confirm the Government's intention to use the ID Cards register in this way while the ID Cards Bill is still being debated and so avoid subsequent criticism, say from the Information Commissioner, that the ID Cards register is subject to 'function creep'".

13 July 2005—Ministers left to decide about informing Parliament

A50. The Project Board sent different recommendations to Ministers ("Submissions to Ministers") and the explicit 30 June text mentioned above was dropped in favour of a simple statement: "it is in the public domain that CIP is due to report to Ministers this summer but no date has been given for a Ministerial response". However, a draft letter prepared for Chief Secretary of the Treasury to distribute to Cabinet colleagues sought responses by 7 September 2005 as "I intend to make an announcement after Parliament returns" (in October 2005).

A51. A draft "Written Ministerial Statement" to Parliament was included as Annex B of this package. This contained sufficient detail to stimulate an informed debate about the merger of the CIP with the NIR if the statement was issued. In the event, no statement was made to Parliament in October 2005; however the draft Statement delivered in Annex B is not significantly different from the Statement which eventually appeared in 18 April 2006 after the ID Card Bill had become law.

A52. The Chief Secretary of the Treasury at this time was Des Browne MP who had also signed the Regulatory Impact Assessment on 29 November 2004, which related to an earlier version of the ID Card Bill. It is not known whether his detailed knowledge of the ID Card scheme played an influential part in the decision not to inform Parliament.

[53] CIPPB(05)45 dated 21 June 2005.

19 July 2005 –ID Card Bill Committee stage (Commons)

A53. In Committee, the Home Office Minister avoided reference to the fact that powers in the Bill were needed to ensure integration of CIP's wide data sharing functionality into the NIR (eg as identified by 24 September 2004). Instead, explanations were provided in narrow terms; for example "In fraud investigations it would be sensible, from its point of view, for it (a local authority benefits inspectorate) to have access to the register" or that "The fire and ambulance services could also be beneficiaries of access when verifying identity against the register following a major accident".[54]

20 July 2005—Response to written question, column 1783W

A54. The following written question illuminates what was to be the "obscure or deny line" adopted by Government with respect to its comments on the use of the NIR for public administration purposes (until after the ID Cards Act received Royal Assent in March 2006).

> **Harry Cohen**: To ask the Secretary of State for the Home Department if he will introduce an amendment to modify the Identity Card Bill so that personal information from the national register associated with the identity card cannot be used by any public authority for the purpose of the efficient and effective delivery of public services without the consent of the identity card holder; and if he will make a statement. [13169]
>
> **Andy Burnham**: The Government will not introduce such an amendment. The Bill as drafted only allows information to be used without a person's consent by specified public authorities named on the face of the Bill, or others subsequently approved by Parliament. These arrangements will be subject to independent oversight.

5 and 18 October 2005 (Third Reading debate)

A55. There were two further Parliamentary opportunities for Ministers to refer to the decision to use the NIR as a basis for the CIP functionality. On 5 October,[55] MPs were told that "Direct access to information held on the National Identity Register by anyone outside those responsible for administering the scheme will not be possible, only requests for information can be made by third parties. In the vast majority of cases, verification of information on the Register will only be possible with the person's consent". During the Third Reading debate on the Bill, on 18 October, the Home Secretary[56] (Charles Clarke) reinforced this message in the House of Commons: "What the Bill allows is for information to be provided from the register either with the consent of the individual or without that consent in strictly limited circumstances in accordance with the law of the land".

A56. It is a challenge to reconcile these two statements, and the answer to Mr Cohen's PQ, with the letter sent to the Home Secretary in September 2004 or the 24 June 2005 minutes which envisaged that, **without** the need for consent of the individual concerned, "basic contact data held on NIR to be downloaded to other public sector stakeholders" or for "basic contact data held by stakeholders can be up-loaded to the NIR".

24 October 2005—Publication of Constitution Committee's Second Report

A57. This Report essentially repeats the First Report, but includes an exchange of correspondence in July 2005 with the Minister. In that correspondence, Baroness Scotland states:

> "Government departments or public authorities may be provided with information from the Register without consent but only if prescribed in regulations approved by Parliament. So it will always be clear which organisations can be provided with data in this way. The Bill also allows regulations to set rules as to how information can be provided in these circumstances, again this will be an open, transparent process".

A58. It is difficult to see how the above tentative text conveys the intend of Government or the firm decisions that **had been taken** (eg as illustrated in the minutes of the final meeting of the CIP since September 2004). For example, the paragraph not clearly represent the fact that "the responsibility for delivering an adult population register that enables basic contact data held on NIR to be downloaded to other public sector stakeholders" (without consent) **had been** incorporated into Government plans for the ID Card scheme.

[54] 19 July, 9th sitting morning, Column 363 (Standing Committee Hansard).
[55] *Hansard*, 5 October 2005, Column 2845W.
[56] *Hansard*, October 2005 (Column 799).

24 October 2005—Joint Committee on Human Rights

A59. The Joint Committee on Human Rights (JCHR) published a report which questioned the access to NIR data via wide ranging powers in the ID Card legislation.[57] It reported that "We consider however that there remains a risk that a number of provisions of the Bill could result in disclosure of information in a way that disproportionately interferes with private life in violation of Article 8". These comments reflect Recommendation 60 of the Home Affairs Select Committee Report into Identity Cards which stated that "It is unacceptable that basic questions about the degree of access to the NIR should be left to secondary legislation".

A60. Both these comments were targeted at the kind of disclosures that were the subject of the legal advice dated April 2003 and were eventually published in April 2006. It is curious that although the Government saw no problem in publishing this legal advice in April 2006, the advice was not made available to inform the JCHR's scrutiny of the ID Card Bill in October 2005—some six months earlier (or indeed the Home Affairs Select Committee).

9 November 2005—The Delegated Powers and Regulatory Reform Committee

A61. The House of Lords Delegated Powers and Regulatory Reform Committee, in its Fifth Report[58] on the Identity Cards Bill, followed other Select Committees and expressed concern at the wide ranging powers in the Bill. In their evidence to the Committee,[59] Ministers did not explain the need for these powers so that the NIR can possess CIP data sharing functionality. Instead they explained that these wide data sharing powers were needed to cope with the exceptional or obscure emergency situation:

> 104 . . . "The more obvious recipients of information from the Register are dealt with explicitly in the preceding clauses, but it is regarded as essential to have a reserve power to use in the public interest if it should be necessary. For example, it is conceivable that the power could be used to specify public authorities that are not Government departments such as the emergency services or local authorities for specified purposes".

A62. Note the use of the phrase "it is conceivable"—far more reaching decisions had been already been conceived months earlier (eg see 24 June 2005).

16 January 2006, Lords Committee Stage—no explanation of CIP functionality

A63. Baroness Anelay of St Johns successfully moved an amendment which replaced the words "securing the efficient and effective provision of public services" with "preventing illegal or fraudulent access to public services". This amendment removed the legal basis for the integration of CIP with the NIR (eg as decided in September 2004).

A64. In her attempt to defeat the amendment in the Lords, the Minister did not take the opportunity to expound the virtues of data sharing or explain that 20% of the business case for the ID Card depended on the merger of the CIP with NIR. Instead, the Minister explained the phrase "securing the efficient and effective provision of public services" in terms of the use of the Card whereas in practice, most of the efficiency gains of the CIP will depend on the use of the database.

> "We should not limit the use of identity cards in helping to deliver better public services. It is not just a question of combating fraudulent use of public services; it is also about helping to transform those services. We believe that the public will want the introduction of identity cards to be used as a way of helping public services to deliver quicker and better services. Why should we have to keep filling in different forms with details of our name and address? If production of an identity card when seeking access to a public service can confirm our identity quickly and easily, surely we should be aiming to provide that. If producing an identity card enables address details to be confirmed, that will help both the public service and the applicant for that service". (16 January 2006: Column 478)

A65. The amendment was overturned by the House of Commons (13 February 2006). There was no Commons debate on the matter because of a guillotine motion, used by the Government, limited debate on Lords' Amendments. This fact alone, in itself, raises important issues of Parliamentary scrutiny.

[57] Joint Committee On Human Rights (First Report), section 4, session 2005–06.
[58] Session 2005–06, 10 November.
[59] Appendix 1 of the above report.

March 2006—a game of Parliamentary ping-pong

A66. The House of Lords and Commons disagreed over the interpretation of Labour's manifesto which promised "We will introduce ID cards, including biometric data like fingerprints, backed up by a national register and rolling out initially on a voluntary basis as people renew their passports". The House of Lords said that this meant that people should be able to choose whether to obtain an ID Card with the passport; the Government said that as people volunteered to get a passport, that the ID Card could be issued to passport applicants. The result was a dispute and the ID Cards Bill ping-ponged five times between both Houses of Parliament.

A67. Eventually, a compromise was proposed by Lord Armstrong, where individuals did not have to have an ID Card if they applied for a passport before 2010, but their details would be entered into the NIR. Accepting the amendment, the Home Secretary told Parliament: "Lord Armstrong's amendment preserves the integrity of the national identity register. It ensures that the details of all applicants for designated documents will still be entered on it. That will mean that they will be afforded the protection that that will provide from identity theft. It will also provide the wider benefits to society by ensuring that attempts by people to establish multiple identities are more easily detected".[60]

A68. The minutes of April 2005 stated that the CIP formed one-fifth of ID Card's business case so long as entry of citizen details into the NIR is compulsory. This had been known for almost a year—however, this reason was not proffered by the Home Secretary in his explanation for accepting Lord Armstrong's amendment.

18 April 2006—Government announced NIR and CIP merger

A69. At the end of March 2006, the ID Card Bill gained Royal Assent without the merger of the NIR and CIP projects being raised. On 18 April[61] an announcement was made to Parliament by means of a written statement which explained that the CIP project had wound up. The April statement is not significantly different from the draft sent by the CIP Board on 13 July 2005—some nine months earlier. There was a comprehensive disclosure of CIP documents on its website which explained in detail the new functionality of the NIR.

15 May 2006—Prime Minister promotes "identity management"

A70. In an open letter, Tony Blair promoted the widespread public administration use of the NIR database. He told Home Secretary John Reid[62] "Eighth, I am keen to maximise the benefits of ID management (ie all transactions where a declaration of identity is required), including the introduction of ID cards by 2009. The full range of activity relating to identity management needs to be co-ordinated across government to maximise benefits to the citizen. I would like you to identify a Minister to focus closely on this and the agenda across Whitehall". Identity management also includes the e-government agenda.

A71. The minutes of this project also shows that there are early links to the use of the NIR in relation to the Government's policy of Identity Management. Transformational Government and e-Gov initiatives (eg see the minutes of the CIP project around March and April 2005). The Crosby Review could add to the use of the NIR in this respect.

October 2006—national identity management confirms use of NIR on the lines of the CIP

A72. The term "national identity management" is being used by Government to include the wider use of the NIR (eg to include a population register as envisaged in the Citizen's Information Project (CIP)). This can be shown by reference to the government's first "*Section 37 report*" on the likely costs of the UK Identity Cards Scheme (published in October 2006). Pages 7 and 8 of this report on ID Card costs (at bottom) reads:

— "Firstly, it (use of the NIR as a population register) would allow organisations to be more proactive—people could be contacted before their passport needs to be renewed; when employees need to fill out self assessment tax returns; targeting 300,000 citizens who are not claiming state pensions or those in particular age ranges who are eligible for health screening; allowing authorities to collect debt from citizens who have moved to another area; and reducing the overall administrative burden on bereaved people".

[60] *Hansard*, 29 March 2006: Column 1000.
[61] *Hansard*, 53WS, 18 April 2006.
[62] http://www.pm.gov.uk/output/Page9461.asp.

A73. This paragraph published **in October 2006** can be compared with the list published on the first page of the Citizen Information Project's final report given to Ministers in **June 2005**.[63] The opportunities of wider use of the NIR for CIP purposes were listed as including:

— Managing passport application peaks by getting customers to apply early;
— Taxation authorities "contacting employees required to complete self assessment";
— "DWP targeting the 300,000 eligible citizens not currently claiming pensions";
— "Local councils collecting debt from citizens who have moved to another authority"; and
— "reducing the overall administrative burden on bereaved people".

March 2007—NIR to be used as a population register

A74. According to Home Office Ministers,[64] as "the National Identity Register is intended eventually to contain up-to-date identity information for all United Kingdom residents aged 16 and over. This will include name, age, address, nationality and biometric information, such as photograph and fingerprints. The National Identity Register will then be able to serve as a United Kingdom adult population register".

A75. It is interesting to note that one of the original Government consultations[65] stated that legislation would be needed to establish a population register and that "this stage will also include public consultation to explore the issues around public acceptability of the proposal". This promised public consultation has yet to occur and this subject has, as far as I can assess, could have and should have formed part of Parliament's scrutiny of the ID Card Act 2006.

Examination of Witness

Witness: Dr Chris Pounder, Pinsent Masons, examined.

Q841 ***Chairman:*** Dr Pounder, good morning. Welcome to the Committee. It is very good of you to come. We are not being televised this morning but we are being recorded, so could I ask you, please, to formally identify yourself for the record, and if you would like to make a short opening statement, please do.
Dr Pounder: My name is Dr Chris Pounder. I am currently employed by Pinsent Masons solicitors, law firm. I have been in data protection for as long as I can imagine, and I am ready to go, so to speak.

Q842 ***Chairman:*** Thank you very much indeed, and thank you very much for the paper which you sent us. Perhaps I could kick off by asking how confident you are that the development of jurisprudence through cases decided in British and European courts, particularly with reference to European Convention rights, can provide effective protection for the personal information of United Kingdom citizens? Is a consistent privacy and data protection jurisprudence in your opinion already being developed?
Dr Pounder: The short answer is I am not confident that Article 8 will provide satisfactory jurisprudence because there are very few cases going to the courts. Those cases that tend to go into the courts primarily involve, as you say, people who have celebrity status, and some of the celebrity status cases involve awkward issues. For example, in the *Douglas v Hello!* case there was a privacy case in relation to one magazine doing a spoiler for another magazine. Article 8 privacy cases I do not think are a satisfactory jurisprudence; it is a sort of celebrity endorsement, but in relation to the other cases, for example, *Marper*, which is to do with the DNA database, I think it is an unequal struggle. Anybody who is trying to take an Article 8 case on has to take on the unlimited resources of the state. For example, in the case of *Marper,* the fees obtained by Marper's team for the whole case, taking it from admissibility to the Human Rights Court was £1,350 whereas on the Home Office side there were 11 lawyers and a leading silk. It is an unequal struggle. What needs to be done, in my view, is a means by which Article 8 cases become more accessible to the public, and it can be done by the Data Protection Act.

Q843 ***Lord Morris of Aberavon:*** Is there no legal aid available for persons like Marper?
Dr Pounder: The legal aid budget is very tight and yes, there is legal aid money. In the Data Protection Act there is this word "necessary", necessary, for example, for a statutory function. The word "necessary" has been interpreted by the courts to have the same meaning as "necessary" in terms of Article 8. So if you made an explicit link between the Data Protection Act and the Human Rights Act, you can use a very simple mechanism in the Data Protection Act to take it to the Human Rights Court

[63] See 24 June 2005 timeline entry "Final meeting of the CIP project".
[64] Answer to Mr Hoban's PQ 127212, 13 March 20.
[65] "Legislation on Identity Cards: A consultation", paragraph 3.20 (CM 6178).

and it makes it more accessible to members of the public. Yes, there is legal aid, but some of the cases do not qualify for legal aid because the legal aid budget is so stressed.

Q844 ***Lord Lyell of Markyate:*** Your written evidence is critical of the weaknesses of the Data Protection Act, and you draw attention to the European Commission's unease about the Act's compliance with the terms of the EU Data Protection Directive. I note you also say at paragraph (g) on page 7 that the Information Commissioner is not a powerful regulator. You point out that he has not all the powers of other regulators. What changes to the Act are required in order to bring it in line with the Directive, and what are the chances of this happening?
Dr Pounder: This might be, in a sense, a red herring, because the European Commission and the Government have disagreements about the Data Protection Directive. In total, 11 articles are under question. What the Commission is worried about, in my estimation, is the meaning of "personal data" following the *Durant* decision, which narrowed the scope of personal data, the extent to which manual files held by the private sector are covered by the legislation, the fact that the courts have assumed that they have an unfettered right to deny subject access in addition to the other exemptions in the Act, and the powers of the Commissioner. I do not know what the problems with the other articles are. There are other reasons for the dispute between the Commission and the Government because no information is being made public. Will these changes come into effect? No, I do not think so, unless the EU start infraction proceedings and the Government, for example, cave in on those.

Q845 ***Lord Lyell of Markyate:*** Can I just follow that up? While I was a barrister I paid £35 a year to register for the Data Protection Act, declaring another interest with a very small business running a house in France where we did not sign up and I am sure we were right not to; it would have been a perfect pest and a waste of £35. What is the real problem here? What is the real mischief that the subject is going to suffer, or is it just another bit of bureaucracy? I may say I am very much in favour of the Information Commissioner. I think he is excellent. What is the real problem with the Data Protection Act? Does it serve a useful purpose?
Dr Pounder: There is no real problem with the Data Protection Act. The real problem is with the structure in which it operates. For example, if you assume that Parliament has a role to scrutinise the executive when it proposes interference with private and family life, you have to assume also that Parliament is informed as to the justification for the various interferences. If you have a Commissioner, for example, a regulator, who has difficulty naming and shaming organisations that transgress the Act, then enforcement mechanism is weak. If you have, for example, a data subject who cannot, shall we say, protect their own privacy, then there is a need to put into the Data Protection Act a right to respect the processing of personal data in accordance with family life, et cetera, in relation to Article 8. That does not disturb the relationship with the press but it does give the ease with which individuals who have a grievance can raise matters with the regulator. So I think it is not the Act that is the problem; it is the infrastructure that supports the Act.

Q846 ***Lord Lyell of Markyate:*** The difficulty of enforcing it.
Dr Pounder: The difficulty of enforcing it and also, for example, when Ministers want to propose legislation in relation to interference, the justifications given to Parliament. This lack of scrutiny causing a great deal of unease.

Q847 ***Lord Norton of Louth:*** I would like to pick up on the point about the Information Commissioner. You have mentioned in your evidence that the Information Commissioner's Office is too limited in its powers to be an effective regulator. What is it that is missing? What would you do that is specific to the Commissioner?
Dr Pounder: This would be a long wish list but I will limit it to four. The first one, I think, is that the Commissioner has to be given the resources to do the job. At the moment £10 million is the money that the Commissioner generates, not from public sources but from registration fees. This compares unfavourably with the hundreds of millions of pounds in the budget of the FSA or the Health and Safety Executive or even the Food Standards Agency. So the ability to do the job is important, but in relation to powers, my top three would be the ability to serve what I would call an Article 8 notice, so if there is a Statutory Instrument enacted by Parliament—and, as you know, SI procedures are not particularly strong—then the Commissioner can by notice approach the courts to strike out a Statutory Instrument, and that would give reassurance to those that perhaps when you have primary legislation which has wide-ranging things, like the Secretary of State may by order do something else, that those powers are not misused. The second one is basically the ability to refer matters to Parliament. Can I give you an example? The Audit Commission has a code of practice going out for consultation at the moment. This code of practice will be laid before Parliament. There is going to be a consultation process with the Commissioner. If there is a disagreement, the sort of procedure that I would like to see is that such a code of practice has to be

approved by, say, a Statutory Instrument procedure by Parliament. That gives the opportunity for the Commissioner to identify what the problems are and the ability to Parliament to identify and take a view as to what public policy should be. It is that kind of mechanism I am looking for.

Q848 ***Lord Norton of Louth:*** So there are powers you would vest in the Commissioner which he does not have at present, and on the resource side, you are talking in terms of giving more resources *per se* but in terms of the specificity of those resources, is one of the problems in relation to the technical know-how that is available to the Commissioner in order to keep abreast of all the changes in surveillance that take place?
Dr Pounder: That might be an issue, but if the Commissioner has resources, he might be able to buy them in. I do understand from what the Commissioner has said publicly that he has difficulty retaining staff that he has skilled up, and obviously that is part and parcel of the resource issue.
Lord Norton of Louth: That is one of the existing limitations, the nature of those committed resources.

Q849 ***Lord Rowlands:*** As you have raised the issue of Statutory Instruments and primary legislation, do you think there could be some value in having a robust privacy impact assessment that any government department drafting legislation would have to, as it were, put that test and publicly announce when that is done, and what for, to identify at the beginning the privacy issues in any Bill or in any Statutory Instrument?
Dr Pounder: Yes, that might help, but privacy impact assessments as currently viewed by the Commissioner are a technique for once you have the project design up and running, to make sure that the project operates within the law and within the data protection regime. Taking a step back, it is justification. I would like, and the Joint Committee on Human Rights has mentioned this, for Parliament to have, say, for example, a Human Rights Memoranda. That is what the Joint Committee on Human Rights want. Also, I am not convinced that the legal advice in relation to a Bill's compliance with human rights cannot be published. The Government published this legal advice in relation to the use of the National Identity Register as part of the Citizens Information Programme. That advice is on the website. If they are publishing that kind of legal advice for, say, the Citizens Information project, it is difficult to understand why it cannot reassure Parliament that essentially it has considered the human rights element practically and this is the legal advice demonstrating how it is compliant with it.

Q850 ***Lord Rowlands:*** Would the value of such an assessment right at the beginning in the preparation of a Bill or of an Order at least flag up to anybody interested in parliamentary terms that they would see that there was an issue or there could be an issue at an earlier stage? All your evidence suggests we do not see it.
Dr Pounder: No, I am not saying that at all. The privacy impact assessment is a risk assessment, and part of the risk assessment is, I would have thought, what the value is of the interference. For example, if you take the Audit Commission code of practice, it said, "Before we do a data-matching exercise we will do a pilot study." It does not say that in the code of practice but it could do: that pilot study could identify the costs involved in the interference, the amount of money involved in the interference, how the interference is done, and the outcomes, so that people could see whether or not the interference was worth its weight in gold or whether the data-matching exercise has worked. I agree with you there is an important stage here in making sure that people take account of the risks, but when the Government takes account of the risks, you have an extra step here in relation to legislation which is that Parliament has to scrutinise. If Parliament is to scrutinise what the Government is saying, and Parliament is going to authorise interference, at least the parliamentary authority needs a fully informed debate. Obviously, a privacy impact assessment could form part of that but it is not what the Commissioner thinks a privacy impact assessment is.

Q851 ***Lord Lyell of Markyate:*** As we know, Ministers put their name to Bills saying they are compliant with the Convention but you are suggesting that their Department should publish an opinion which indicates that it has considered the issues, the pros and cons, and setting out the legal reasons why it thinks it is compliant. It sounds a good idea to me.
Dr Pounder: Absolutely. I think the Joint Committee on Human Rights has actually expressed that, and from what I understand, the Joint Committee on Human Rights is going "quietly spare" that it has not been done.

Q852 ***Lord Morris of Aberavon:*** On the same point, these statements of compliance with the Convention are made. Are there any examples in your field where, the statement having been made, it is found subsequently that they are not in compliance?
Dr Pounder: It is very difficult. Say, for example, the identity card legislation. As you know, it is a paving Bill with wide-ranging powers. The only way to challenge in human rights is, first of all, to have a Statutory Instrument, then somebody to put their head above the parapet to take a human rights case.

It is a long way down the chain. If you look, for example, at the *Copland* case, which I thought was "slam dunk", the *Copland* case was the woman from a West Glamorgan further education college, and her communications were interfered with. The case was well before RIPA, yet it took round about eight to ten years to get to the Human Rights Courts, by which time it is too late. What you need is something more immediate, more accessible. If somebody can raise a valid human rights case, I can go to the Information Commissioner and say, "Look, I think this is unlawful because of so-and-so," and if the Commissioner agrees, he can start a mechanism that could strike the order out.

Q853 ***Lord Morris of Aberavon:*** What you want is an early mechanism to prove the value of the ministerial assurance.
Dr Pounder: Yes, absolutely. There are a lot of parliamentary Committees, certainly the Joint Committee on Human Rights, saying "We can't perform our scrutiny job if we don't have this information." Ministers argue that you do not need to worry about the Statutory Instruments because if they get it wrong, the courts will strike them out, but who is going to put their head above the parapet and when? Ten years down the line. Such litigants are going to put their house on the line against, for example, the unlimited resources of the taxpayer. It is an unequal struggle. There needs to be something far more accessible where these things can be tested. I am quite happy for Ministers to say, "Look, I don't need to bother Parliament about the detail but if we get it wrong, the SI is going to be struck out" if there is an easy mechanism whereby that can be challenged. The ability of having that mechanism would mean, I think, that civil servants would be very mindful of the Human Rights Act when they drafted their Statutory Instrument because they would not want the Commissioner to strike it out.

Q854 ***Lord Smith of Clifton:*** Dr Pounder, in your evidence you gave a detailed case study of how scrutiny of the purpose of the National Identity Register was in effect prevented by Ministers. You say that this raises a constitutional question about the Government's plans for this database. Without rehearsing the NIR case, could you please elaborate on this view and explain how the case "raises questions about Parliament's ability to scrutinise any legislation effectively"?
Dr Pounder: Just to go into the history, when I wrote that analysis, I became more and more shocked as to the discrepancies between what Parliament was told and what the officials had decided. I do not know whether it is deliberate or not but I just reported the facts to the Department. What is the use of the NIR for a public administration purpose really about? It is about efficient and effective public services, yet Parliament was—how shall I say—not informed as fully as it should have been. If you go back over the years and if you look at, for example, Supergun, Matrix Churchill, the war in Iraq, BAe, what should Parliament be informed of? Those sorts of cases have a problem—it may be trade, it may be national security, it maybe foreign affairs overtones which make it difficult for Ministers to respond. The worry for me is that my evidence on the NIR and public administration is that there is nothing about national security, nothing about foreign affairs; it is about effective public service delivery. There should be no prohibition on releasing information to Parliament. So now we have two extremes. If, for example, it is something like Supergun, one where Parliament is not informed, then essentially, in relation to the NIR uses for public administration, Parliament is not informed—what happens to everything in the middle? That is the question it raises. That is the reason why I say it does raise this particular question. My own view is that Ministers drip-feed information to Parliament when it is appropriate. For example, in that evidence I showed that there was a written statement prepared just after the General Election which was not published for nine months, a written statement saying the NIR would be used for public administration purposes. Before the Bill came before Parliament, the Government knew that 20 per cent of the business case for the identity card relied upon the use of the database for public administration purposes. They knew that the identity card had to be compulsory to get that 20 per cent. I have not found any ministerial statement, apart from the written statement that was produced after the legislation passed through Parliament. This Constitution Committee was worried about the relationship between the state and the individual in relation to the NIR and published two reports. Did it know that the Government were planning to use the identity card database as an information resource? The other fact of course is David Blunkett had produced two public statements, documents of 150 pages each, which assured members of the public that the database was not going to be used for this purpose. There are lots of constitutional issues around this, and what I would like you to do is not see that evidence as knocking the use of the NIR as a public information resource or a population register. I think there are good arguments for it. What you should look at is how Parliament was informed, if Parliament was not informed, how can it scrutinise?

Q855 ***Baroness Quin:*** Just following up the question relating to scrutiny, the evidence in paragraph 17—this is written in May 2007 –talks about "the next Prime Minister has signalled his intention to grant parliament more powers of scrutiny." Presumably,

the next Prime Minister was Gordon Brown at that point. Has anything happened, and in what context was that commitment given?
Dr Pounder: The draft Constitutional Renewal Bill is now being debated. I think the Prime Minister gave a speech where he said that he was looking at the ability to balance the two. That is why I picked up on that speech saying proposals would come forward, which I assume now is the draft Constitutional Renewal Bill.

Q856 ***Baroness Quin:*** Is there anything in there that gives you comfort?
Dr Pounder: No, not on this particular issue. We are talking about general interference and the ability of the executive to be scrutinised. Parliament has to have the information to allow that scrutiny to occur. That is what I am really worried about. I see nothing that requires Ministers to provide information to Parliament. Yes, they will give assurances; yes, there might be problems in producing certain information, but Parliament has committees that deal with sensitive matters and there are always sensitive data procedures. But the fact that information is, shall we say, withheld from Parliament on something as mundane as public administration I think is shocking, to put it bluntly.

Q857 ***Lord Rowlands:*** On first reading the appendix to your evidence I thought it was a devastating critique. This is over a year old. Has there been a rejoinder? Have they engaged you in argument or debate on your assessment?
Dr Pounder: No. All I laid out was the evidence. I tried to withhold the comments that I could have made.

Q858 ***Lord Rowlands:*** There has not been a response to this?
Dr Pounder: There has not been a response. I do not know whether there has been a miscommunication between the civil servants and Ministers but I think the evidence should be seen as, is this how Parliament is treated for every single thing? It is rather as if Parliamentary management and news management are the same thing.

Q859 ***Lord Peston:*** I am still a bit lost on this. Like Lord Rowlands, I was very impressed with the criticisms you offered but, as a long-time supporter of identity cards—and I declare an interest—it seems to me obvious that identity cards, to be of any use, have to be compulsory and the notion of an optional identity care seems to me ridiculous, but equally, I had always assumed that the identity card had both a public sector side to it and a private sector side, because a great deal of a person's life dealing with private sector matters is establishing who they are. Given that, and ignoring totally the fact that people like me thought it was going to be a simple scheme—and it has got so complex that we all know it is going to be a disaster—what troubles me is this business of Ministers, in a sense, misleading Parliament. Is not the purpose of the register perfectly obvious? What is the Government concealing here? I put this to you to raise the difficulty: what do you want the Government to be saying to us, if you like? What information are they withholding from us?
Dr Pounder: They are not withholding information; they are just revealing it at a time which is very convenient for the scrutiny process. To go back to the Written Statement, it was prepared before the Second Reading of the Identity Card Bill. It could have been issued. Parliament could have debated whether or not the National Identity Register should be used for public administration purposes but that was withheld for some reason.

Q860 ***Lord Peston:*** Unless you assume that we, both in our House and in the Commons, are a bunch of complete idiots—which is not an impossible assumption to make—why does someone not just get up and say it?
Dr Pounder: That is the point I am making.

Q861 ***Lord Peston:*** There is nothing stopping them. You are criticising the Government. Why is no Member of Parliament in either House getting up and saying "Isn't it obvious what this is for?"
Dr Pounder: It has been obvious to me for a very long time what the NIR is for but the public statements are completely the opposite. If you go back to the identity card, look at David Blunkett's original paper, asking should we have an entitlement card, it stated categorically that the population register was a different system. The Government said the systems were really quite difficult. I think there is a perfectly good argument for using the NIR as a population register. The point I am making is, let us have that argument as part of the identity card project when the legislation is going through, because that is when the decision was taken to do it.

Q862 ***Lord Peston:*** You are really accusing Members of both Houses of not quite doing their own job. Both Houses actually contain some very able people who could take Ministers apart with ease.
Dr Pounder: The obligation on government is to subject to scrutiny. That is the point. Yes, we can argue the pros and cons outside but it is the fact that it is not one instance. There have been a number of instances where Ministers, I should say, struggle to be economical with the truth.

Q863 ***Lord Lyell of Markyate:*** I am really trying to get at what you think the mischief is here. I perked up when you talked about Supergun and Matrix Churchill because I had some involvement in those. I do not know whether you can illustrate it with those two examples. Start with Supergun: did Ministers know something or did civil servants know something which they did not tell Parliament about? What is the point that you are making?
Dr Pounder: I cannot go back; I cannot remember Supergun. I would have to get out the Scott Report and thumb through the 20 volumes. The mischief is essentially this. If government say that they are not going to use the National Identity Register as a public information resource, you have to take that at face value, but behind the scenes they decide they are going to use it as a public information resource, and they prepare written statements to Parliament—the civil servants do this—which are not released for some reason. How can you have an informed debate if that sort of thing is happening?

Q864 ***Lord Lyell of Markyate:*** I understand that. Just go on. Do you think we should be frightened if they did both say and use the NIR as a public administration resource? Is that a frightening thing or not?
Dr Pounder: It depends how it is done. If you are going to share information, there are essentially three ways you can do it. The first way is with consent; the second way is by statutory requirement, in which case you do not need individual consent; and the third way is you have a statutory gateway but you allow an easy mechanism to object. Those are the only three ways you can do it. What the Government have done is said, "We are going to share information for public information resource without the consent of the individual concerned." That is what their legal advice says on the website, on the CIP website, so they have taken legal advice to use the identity card database as a public information resource without the consent of the individual concerned. My belief is this: when can the state interfere with private and family life? Crime is one, national security, there is a whole list, but public administration in my view is not in that list. If Parliament takes a decision to do the latter, then of course we can engage the parliamentary process, but if Parliament is not informed of the decision, lo and behold, it is going to go ahead willy-nilly, using Statutory Instrument powers some time in the future.

Q865 ***Lord Morris of Aberavon:*** It is basically a question—and I am not coining the phrase—of the Government being economical with the truth.
Dr Pounder: Very economical with the truth, I think.

Q866 ***Lord Morris of Aberavon:*** You improve my question!
Dr Pounder: This is why I am quite keen on, for example, the ability to link human rights and data protection explicitly, so that if these powers are used in a way that some people may feel detrimental . . . Remember, you can only scrutinise the proposals before you. The human rights is implementation. If the implementation does not mirror, then somebody can easily take a human rights case through the Data Protection Act if you link the two together explicitly, which I think is something that would be very valuable.

Q867 ***Lord Morris of Aberavon:*** I am going to take you up on the role of primary legislation and secondary legislation. The Joint Committee on Human Rights criticised the Government's approach to this on data sharing. There is nothing new in this. We have always operated on general clauses to be implemented but if they go well beyond the assurances they gave, that is a matter that is suspect. I have been furnished with a letter from Charles Clarke, who was then Minister of State when the RIPA Bill was going through, where he gave categorical assurances to Bill Cash, MP: "I can confirm even at this stage that such powers will not be available to local authorities." Lo and behold, in 2003 such powers were given to local authorities for the purposes of preventing or detecting crime or of preventing disorder. Whether they have kept to that remit is another matter. Do you share the concern of the Human Rights Committee and what would you do yourself?
Dr Pounder: I do share the concern of the Human Rights Commission. Is it the Human Rights Committee or Commission?

Q868 ***Lord Morris of Aberavon:*** It was the Joint Committee on Human Rights in their 40th report.
Dr Pounder: I do share their concerns and I do think they are right. I think Parliament needs to be more informed and more involved. I do worry about Ministers arguing "Don't worry about these Statutory Instruments. We will get it right and they can be struck out." For example, in the case of Poole, if there was an ability for the Commissioner to serve, for example, a human rights notice and test whether or not the interference was necessary in accordance with RIPA, the matter can be resolved in that particular way.

Q869 ***Lord Morris of Aberavon:*** Is Poole a unique example, or is it one of many? We have had witnesses here, senior officers of local government, and they swear they take a proportionality test, and it is done at a certain level, something akin to a superintendent in the police force. Is Poole a glaring example of something well beyond preventing or detecting crime?

Dr Pounder: Crime is milk bottle theft and murder, is it not? It is proportionality. It is on the cases. Yes, you can have officers assessing proportionality, but who assesses whether or not the officer came to the right balance? It is back to that particular point again. If you have a single point of contact who identifies the balance between the investigator and the interference—interference and non-interference—but that authorisation officer in a sense sometimes makes mistakes, obviously. We are all human, but there is no mechanism apart from somebody taking a case under the Human Rights Act for the way those officers who make the assessment make the assessment in accordance with the human rights obligations. There is no way of checking that simply, cheaply and effectively.

Q870 ***Lord Morris of Aberavon:*** We have got the point of the need for a mechanism to check but my earlier question was is Poole a unique example or do you know of any more? It seems to me deciding whether children are going to the right school, or whether the dustbin is only partially open when it should be shut, does not seem to me to be detecting crime or preventing disorder.
Dr Pounder: It could be an environmental crime. I do not know. This is the sort of area where you do need an extra tier of counterbalance.

Q871 ***Lord Peston:*** I am sure from listening to this Committee for the last few weeks that we very much take the proportionality point, particularly in the Poole case, which I think we would all agree was disproportionate, but would it not be equally disproportionate to take that particular mistake to court under the Human Rights Act?
Dr Pounder: Absolutely.

Q872 ***Lord Peston:*** In the end, is the answer not both to publicise the case in the hope that the point gets across and then to shrug and walk away?
Dr Pounder: That might be the correct solution but let us say, for example, if the individual concerned had been damaged in any way, they would obviously want some kind of redress.

Q873 ***Lord Peston:*** Even then, are you sure that is right? You are a lawyer and I am not. My experience of life is that I have been damaged over the years several times when I have felt a grievance, but in the end, you win some, you lose some. That is my attitude to life. We do not want to encourage people to litigate on every occasion.
Dr Pounder: No, absolutely, and the ability to go to the Information Commissioner to ask for an assessment means it might not even get to the courts.

Q874 ***Lord Morris of Aberavon:*** It is the mechanism you want.
Dr Pounder: It is the mechanism, the counterbalance mechanism, yes.

Q875 ***Baroness Quin:*** In your written evidence you state that a major problem lies in the fact that the public body or Minister responsible for policies, procedures that require interference with private and family life can also establish policies and procedures which protect the public from over-zealous interference. So you seem to see the problem of Ministers acting as both prosecutor and defender in this domain. How keen are you on the separation of these two roles? How do you see that separation being reflected both in government structures and in parliamentary procedures?
Dr Pounder: I am very keen that the more severe the interference, the wider the separation should be. For example, in the context of, say, national security cases, I would prefer a mechanism via the courts rather than, for example, the Home Secretary signing off on warrants. One of the interesting things with, for example, the communications warrants and things, there are about 2,000 signed each year, and if you look at the parliamentary evidence, Home Secretaries down the ages will say "We take this very seriously." I am sure they do but if you have 2,000, that is around about ten per day and if you are going to take something seriously, are we saying there is a signing ceremony? Just look at the mathematics of it. My own view is that to have separation, I think the Commissioners should report to Parliament on various issues. For example, the ID Card Commissioner will report to the Home Secretary and the Home Secretary will report to Parliament. I think a much better mechanism would be that the Identity Card Commissioner reports to a Committee of the House, the Committee of the House decides what is published following advice from the Government, the Committee of the House could ask a Commissioner to do, shall we say, an investigation into various things to inform the public debate as to what the correct balance is, whereas at the moment the two things can be quite incestuous. For example, the appointment of a Commissioner: at the moment often the Home Secretary and the Prime Minister appoint the Commissioner. I have no difficulty with that but it might be more balanced if a Committee of the House interviewed people who were recommended by the Commissioner and a Committee of the House appointed the particular Commissioner. It would then be much more clear that Parliament is informed in the process. There are quite a lot of things that need to happen in Parliament. The other issue is with Statutory Instruments; for example, I would like the ability for Statutory Instruments to be amended, so that if there

was something contentious, Parliament can have an informed debate. The whole mechanism is that Parliament has to have the ability to scrutinise the executive. That is, in a sense, the thrust.

Q876 ***Lord Rowlands:*** You bring up this business about a potential conflict of interests when the Department is both interferer and defender. Would not the best idea be to embed the whole concept of privacy consciousness in each and every Department with privacy officers, the PIAs and the rest of it? Would that not be the best way to cure the problem, not the symptom?
Dr Pounder: I think recent security lapses have shown there is a cultural problem, and there is a government data handling review, from which I understand—it has not been published yet but I understand that each Chief Information Officer of each Department would have the obligation to make sure that basically procedures are followed. The difficulty is essentially whether that becomes a tick-box operation. Say, for example, with privacy impact assessments, you can see it becoming a part of the bureaucratic process: privacy impact assessment, box ticked, done that. It has got to be something more robust.

Q877 ***Lord Rowlands:*** When we were in Canada the Canadians did not believe that their Information Commissioner should be both responsible for freedom of information and also privacy; they thought it should be divorced. Do you think there is a problem with the Information Commissioner wearing these two hats?
Dr Pounder: I have never been a fan of him wearing two hats, to be honest. I think there is a conflict. When the Information Commissioner got the FOI-type responsibilities, I was thinking that there was a conflict between the two, and if there ever is a conflict between the two, there has to be some publicly transparent way of resolving that conflict. That was my own view.

Q878 ***Lord Rowlands:*** You are the first witness to say "yes" to that argument.
Dr Pounder: Yes, we are a declining species. I have not been a fan of it—I put it that way—but it seems to work when there is a stressful situation. I do not know what arguments go on inside the Commission but where there is a conflict, the resolution of that conflict has to be in the public domain, and separate bodies would allow that.

Q879 ***Lord Lyell of Markyate:*** Could you please explain the recommendation concerning parliamentary scrutiny of secondary legislation as discussed in your second principle, the approval principle? The approval principle seems very sensible on its face, but you go on to say that to strengthen the scrutiny, Parliament could permit a Select Committee to take privacy under its remit. How could this help to overcome the expansion of data collection that results from the current piecemeal approach to legislation? Are there some other measures which might be helpful in this regard?
Dr Pounder: I do not think it would do anything for the expansion, as you mentioned in the question, but it would make it more accountable. Remember, that approval principle follows back behind the justification principle, the fact that government is open in relation to information about its proposals, and then the approval principle is basically for Parliament to challenge the assumptions of government. That is what the mechanism is. If you have that mechanism, then the data sharing arrangements that are contentious would become less contentious if there had been an open debate about the pros and cons of the subject matter. Remember, the other thing that I mentioned was that approval assumes that Parliament has the mechanism to get the information it needs to do the debate, basically, about their particular mechanism.

Q880 ***Lord Lyell of Markyate:*** It seems to me to wrap in with your point that one is allowed to collect data for very broad principles, like better public administration: how long is a piece of string?
Dr Pounder: Absolutely. One of the problems, for example, with the Data Protection Act is that it is purpose-orientated, so the principles are relevant to a purpose. If you have a purpose as broad as public administration, then of course, the principle is more or less wished away. What is relevant to the purpose of public administration? When you look at data protection issues, the key thing is not whether the police should get information about terrorists; it is how it is done, and how it is done is in the level of the fine detail. Basically Parliament is not necessarily equipped to deal with this level of detail when it is dealing with the actual legislation. The "how" is the implementation. If Parliament is fully informed, if you have regulators that can report to Parliament about particular issues, then Parliament can scrutinise the "how" as well as the "whether", if you see what I mean. Of course, the fact that Parliament can scrutinise it may give the thing full legitimacy. If it is done in an underhand way and nobody knows and it comes out from the blue two months later, people say "Hang on a second, what is happening here?" Remember, if people do not trust public authorities, they are not going to provide information to them. They are going to be economical with the truth. If a public authority wanted my telephone number and I did not want to give it, I would give somebody else's telephone number. That is the sort of thing that would happen, because basically, the public have to trust the public

authority, and part of that trust is effective parliamentary scrutiny of the process, which I am not a hundred per cent sure occurs at the moment.

Chairman: Dr Pounder, thank you very much indeed for joining us and for all the evidence you have given, which has been extremely illuminating for us.

Supplementary memorandum by Dr C N M Pounder

WAS THERE SCRUTINY OF SECTION 1(4)(e) OF THE ID CARD ACT?

I have decided to distil my long written evidence to identify some important instances where Parliament and public did not have the chance to scrutinise the use of the National Identity Register as a population register when the ID Card Bill was before Parliament. Because Ministers are to formally respond to my evidence, I thought it useful to identify the sections of my evidence which I think are important. I have no objection to this additional note being sent to relevant officials.

(a) *What was the nature of the debate concerning section 1(4)(e)?*

Section 1(4)(e) of the ID Card Act 2006 permits use of the National Identity Register and authorises interference with private and family live in terms of "the purpose of securing the efficient and effective provision of public services". At the time of the Bill, there were two interpretations of the effect of this provision:

(1) A limited interpretation that permitted the use of the NIR **in support** of the ID Card Scheme objectives. For instance, by using the NIR to check the validity of the ID Card and thereby secure efficient and effective delivery because only those who are entitled to public services receive them, or by case-by-case access to the database to resolve specific problems.

(2) A wider interpretation that **additionally** permitted using the **National Identity Register (NIR)** as a population register to **secure efficient** public service delivery by allowing general data sharing of contact data from the Register (this is the CIP functionality).

In his oral evidence, the Minister said I was wrong and claimed that both interpretations (1) and (2) are on the face of the Bill and apparent to any reader. This completely misses the point. My main point is that interpretation (1) was the only one put to Parliament and the public and during the public consultation about the "Entitlement/ID Card". For example, the Minister, Andy Burnham, in the Third Reading debate on 18 October 2005 stated:

> "Clause 1, with which we are preoccupied, sets out the purpose of the national identity register, and I would tell the right hon Member for Suffolk, Coastal (Mr Gummer) that two very clear statutory purposes for the Bill are given in that clause: first, to provide a convenient method by which individuals can prove who they are—he recognised that he might indeed welcome that—and, secondly, to provide a secure and reliable method by which public bodies and others can ascertain identification and thereby better serve the public interest".

By contrast, interpretation (2) was **never debated** even though it was a central plank of Government policy and Ministers and their senior officials knew this. Somehow, the public and Parliament were denied the information that would have lead to the opportunity of an informed debate on the extensive use of the NIR as a population register as part of the ID Card framework.

(b) *What was the "hidden" Citizen Information Project (CIP) functionality?*

It will also be useful to summarise the extent of the "hidden" functionality associated with interpretation (2) as described in the CIP minutes of **October 2004 to July 2005**. These show that the Home Office, prior to any Parliamentary scrutiny of the ID Card Act 2006, had:

— "the responsibility for delivering an adult population register that enables basic contact data held on NIR to be downloaded to other public sector stakeholders" (The "Treasury and Cabinet Office should ensure that NIR delivers CIP functionality as planned"); and

— "the responsibility for ensuring from around 2021 basic contact data held by stakeholders can be uploaded to the NIR" and to "design the take-up profile of the NIR to be such that population statistics can be realised for the 2021 census".

Additionally, **in October 2004**, Ministers were informed that adding CIP functionality to the NIR improved the Value for Money of the ID Card scheme, and the minutes identified CIP functionality as forming about one fifth of ID Card's business case. It also notes that Ministers were informed that to realise this saving, registration on the NIR (ie and by implication the ID Card) **must** be compulsory.

Finally, I should comment that currently the functionality associated with interpretation (2) is very much on the back burner as Government focuses on delivery of the security aspects of the ID Card. However, the delays in implementing the CIP functionality does not provide excuse for not informing Parliament about the Government's intentions to use the NIR as a population register.

(c) *What are the issues that raise questions that need an answer?*

There now follows a dozen issues: I think issues (2), (4), (7), (8) and (11) are the most important.

(1) Legal advice was obtained in April 2003 and published in April 2006. **The Government should explain why this legal advice which covered the use of a population register (as incorporated into the NIR in October 2004) could not be shared with Parliament when the ID Card Bill was being scrutinised, yet it could be published within 20 days of the ID Card Act being enacted**.

(2) The public consultations held in 2004 said the NIR would not be used as a population register. "Legislation on Identity Cards" (CM 6178), for example, described the population register under a Chapter entitled "Wider issues **not** included in the draft legislation" (my emphasis). **The Government should identify the public or Parliamentary statements that explained to the public, whilst the ID Card Bill was before Parliament, that a population register was now** included as part of the ID Card Scheme.

(3) Paragraph 3.20 of CM 6178 also promised the use of the NIR as a population register would "include public consultation to explore the issues around public acceptability of the proposal" so that any new "legislation would also introduce concrete safeguards for the public". **The Government need to explain why, in the context of the use of the NIR as a population register, this commitment to public consultation around "public acceptability" or "safeguards" did not occur**.

(4) A letter dated 10 September 2004 stated that the merging of CIP into the NIR would "strengthen the VFM case for ID Cards". The minutes in October 2004 report that: "Home Secretary to write to cabinet colleagues . . . including the purpose of supporting greater public sector efficiency". **As the efficiency savings account for 20%, the Government need to explain why it is omitted from ANY Regulatory Impact Assessment (published on either side of the General Election), or in information or briefings given to Select and Standing Committees**.

(5) The letter dated 10 September 2004 also points out that recommends that "the NIR should become the national adult population register long term (but only if ID Cards become compulsory)". **The Government needs to explain why, in all the debates about compulsory ID Cards, the argument that "the ID Card must be compulsory in order to realise CIP efficiency benefits of 20% of the cost of the ID Card Scheme" was not put forward**.

(6) Although this is not a "governmental issue", Ministers need to explain why the wider use of the NIR was not captured by Labour's manifesto for the 2005 General Election—especially as 20% of the ID Card's business case was being justified on CIP's functionality.

(7) **Ministers need to explain why in July 2005, a draft "Written Ministerial Statement" informing Parliament about the wider use of the NIR as a population register was delayed until 18 April 2006 (after the ID Card Bill had become law), when both the Draft Written Statement and the actual Written Statement are not significantly different**.

(8) On 30 June 2005 draft recommendations from civil servants stated: "Urgent—Home Office believe there would be advantages in making an announcement before Parliament rises on 21 July so that the Government's intention to use the ID Cards register in this way is confirmed while the ID Cards Bill is still being debated". Paragraph 17 added "that would confirm the Government's intention to use the ID Cards register in this way while the ID Cards Bill is still being debated and so avoid subsequent criticism, say from the Information Commissioner, that the ID Cards register is subject to 'function creep'". **Ministers need to explain why the civil servants most closely involved in the CIP project formed this view, if it is obvious that the population register functionality is self evidently on the face of the Bill**.

(9) When the ID Card Bill Committee stage (Commons) Mr McNulty responded to a question: "Did he say that the local authority registrar of deaths would automatically access the database to inform it of the death of a citizen?". In column 78, the Minister answered: "The registrar would not access the database, but inform in normal fashion—once the system was up and running—about deaths that needed to be added to particular

records. The registrar would not have access to the database". By contrast the CIP minutes say the Home Office have "the responsibility for ensuring from around 2021 basic contact data held by stakeholders can be up-loaded to the NIR". **The Minister needs to explain this apparent discrepancy (given that the Registrar of Births, Deaths and Marriages are now part of the same department rolling out the ID Card)**.

(10) In Column 346, examples of wider use of the NIR consistent with section 1(4) were given. These were: "A provision could be made for the Department for Work and Pensions to receive information in connection with its fraud investigations", "the provision might be used is to provide the Department for Constitutional Affairs with information to ensure that fines are issued to the correct person, or to provide information about addresses that might be helpful in tracking down individuals who have not paid fines" and "the measure might be used is to provide information to the Department of Health when a patient who is admitted to hospital cannot identify themselves". In column 363, it was "The fire and ambulance services could also be beneficiaries of access when verifying identity against the register following a major accident". **Ministers need to explain why these case-by-case examples of use of the NIR were given preference over widespread use of a population register that would save 20% of the ID Card costs**.

(11) On 16 January 2006 Baroness Anelay of St Johns successfully moved an amendment which replaced the words "securing the efficient and effective provision of public services" with "preventing illegal or fraudulent access to public services". This amendment removed the legal basis for the integration of CIP with the NIR. In her attempt to defeat the amendment in the Lords, the Minister did not take the opportunity to expound the virtues of data sharing or explain that 20% of the business case for the ID Card depended on the merger of the CIP with NIR. **Ministers need to explain why it did not oppose the removal of section 1(4) in terms that its removal would mean that the efficiency gains from wider use of the NIR would be lost**.

(12) In the final stages of the ID Card Bill, there was a lengthy game of Parliamentary ping-pong over the wording of the ID Card commitment in the Labour Manifesto (which only referred to the security, immigration and law enforcement agenda; see paragraph (6)). A compromise solution was reached which included compulsory registration on the NIR but an option not to obtain an ID Card until 2010. **Ministers need to explain why no mention was made that this compromise would also maintain the CIP efficiency savings via the use of the NIR as a population register**.

13 July 2008

Examination of Witness

Witness: PROFESSOR JANICE MORPHET, examined.

Q881 ***Chairman:*** Professor Morphet, can I welcome you most warmly to the Committee. Thank you for coming. We are not being televised this morning but we are being recorded so could I ask you, please, to formally identify yourself for the record.
Professor Morphet: I am Janice Morphet.

Q882 ***Chairman:*** Would you like to make a short opening statement?
Professor Morphet: It may help the Committee to hear a word about my experience before we start. I have been employed in local and central government for nearly 40 years—40 years next year—and during that time I have worked for a variety of local authorities—county, district, London borough. I have been chief executive of a small unitary authority, Rutland, and during the period between 2000 and 2005 I was a local government adviser in what is now CLG, working in e-government and working on local government modernisation. By profession I am a town planner.

Q883 ***Chairman:*** Could I begin by asking whether you think that the modernisation of local government needs a large expansion in the amount of personal data that is collected and shared between departments? If you do, should this be done on a need-to-know basis and a judgement about proportionality, or do you think collections of data should be widely available to many service departments?
Professor Morphet: I think the modernisation of local government has been about using what is collected better and more efficiently, so I am not sure that I would support the view that it entails an increase in the use of data collection. Perhaps I could illustrate that in a particular way. One of the main responsibilities of a local authority is to provide people with benefits through their arrangements with the DWP, and that information at the moment is collected separately by different departments inside the local authority. If you look at a modernised local government perspective, what you clearly see is that many citizens are not actually receiving their full entitlements. There are just over 50 different kinds of financial benefit that a citizen could be entitled to, and work that we undertook when I was in CLG demonstrated that 80 per cent of the information required for those applications for benefit was the same. The current system would be that a citizen would have to fill in as many forms for these benefits as they thought they were entitled to, but a

modernised local government approach would suggest that you collect the information once and, with the citizen's consent, you see if they are entitled to other benefits. That is the first thing to say. I am not sure if the Committee is aware of something called the "T" scheme, "T" meaning trust.

Q884 ***Chairman:*** Please expand.
Professor Morphet: There is a system called the "T" scheme, which is owned by the Cabinet Office, although run independently but certainly linked with them, and what this does is identify perhaps seven levels of risk in terms of their relationship to particular transactions. Most local authorities only get to about level three. If I could illustrate what the levels mean and go on from there, for example, a level zero would be a citizen being issued a library book. There is a very little risk in the loss of a library book. Yes, there is a cost but it is a very low risk. Nevertheless, you have to identify yourself to the local authority before you are permitted to take out a book. Going up the scale, obviously, registering for a service, you might need to provide more information about your identity and that is verified by the local authority. That may be level two. I am just trying to think what might be a level two service. If you are seeking maybe to have a taxi licence, you might argue that that is the middle level. For the upper level, where the risk is highest and where the personal information you have to provide, which is proportionate to the risk of fraud, say, or misuse of public resource, then clearly that is level three. So it goes on to higher levels, which local authorities do not use. The purpose of these levels is to identify clearly for each transaction in local authorities, and indeed in central government, what kind of risk is proportionate and related to each of these transactions, what kind of information needs to be collected, and what kind of staff training and data handling processes go with this. Local authorities are using this approach, which I think is quite cautious, quite responsible, in terms of their use of information. At the upper level, level three, local authorities are of course governed by the DWP's verification framework. Again, I am not sure if that is something you are aware of. Local authorities are inspected regularly by the DWP in terms of their application of the verification framework. For example, if you live in London and you want to get a parking permit to park your car outside your house, you have to demonstrate to the local authority before you receive that permit that you are indeed a resident and indeed that you own the car. There are two proofs that you have to show. However, for a renewal you only have to confirm that that information is still correct, whereas if you were going back for a financial benefit, where the risk of fraud is higher, you have to show the documents *ab initio*. I hope that explains the kind of system that exists.

Q885 ***Chairman:*** Can I just go on and ask whether you think the safeguards against the loss or misuse of personal data by local authorities are adequately developed?
Professor Morphet: The framework which I have outlined to you is used and in force and inspected regularly. I think there are adequate safeguards for those approaches. Clearly, if you look at breaches and information loss in local authorities, I do not think we have had the same kind of issues that perhaps there have been in other public bodies. I think the concern from a local authority's point of view is very much about whether a citizen is being disadvantaged if information is not shared. I am not arguing that information should automatically be shared, but I think there is also a concern that the citizen might be losing out in terms of entitlement and often the citizen does think that the information is shared within the local authority—that is a commonly understood public perception—but it is not and authorities do keep that information separate unless there is a very specific approach and agreement from the citizen to share it.

Q886 ***Chairman:*** Can I ask if you think that the increasing use of information and communication technologies by local authorities presents dangers to individual privacy, or do you think the technologies are designed or could be designed in ways that safeguard privacy?
Professor Morphet: I think the ICT systems that are used by local authorities have really replicated the kinds of systems that we had with paper systems, which I think have these safeguards, because information is not shared. It is held very tightly within the authority and access, say, for example to personal data in social services or children's services now is very tightly controlled. When I was a chief executive, we had an extremely difficult case concerning a family and child protection issues, and certainly I was never allowed to see the case files because they were confidential, and I think those practices are very much steeped in local authority working. I can only speak in terms of local authorities for that, but certainly I have never felt—in fact, I think the danger is almost in the other direction, that people are very frightened of sharing any information and, as we have seen, sadly, with child protection cases, and distressing cases recently, that inability to share and that cultural concern about sharing information has obviously put children at risk. So I think that my view of local authorities would be very much a culture of not sharing information unless there is a very specific code and framework for doing so.

Q887 ***Lord Peston:*** My question follows on more or less from everything you have just said. Could we first of all clarify what one should have in mind when we are talking about data sharing? It seems to me there are several possibilities. One is talking about data sharing within an authority, and then there is data sharing between an authority and something else, and the word "sharing" can either mean you having access to my data or you and me and exchanging data. Could you enlighten us on whether they are all important?

Professor Morphet: I think the three examples you have given are used in different ways. For example, when I was running a local authority, in our Housing Benefit service we did not give housing advice directly; we subcontracted that to the Citizens Advice Bureau, and obviously the staff who then may have needed access to some personal information related to the individual to give that advice had to go through the same kind of training and be subject to the same kind of controls as if they were our own staff. There was no reduction in that standard because another agency was undertaking it for us, and that indeed would be the case. I have had out-sourced services, say, for benefits and the staff who work for Capita or other big companies are subject to the same kinds of standards as your own staff and have to be trained and inspected in the same way. So that is in terms of personal data. If you are thinking about data matching, which is when you are comparing large bundles of information between local authorities, only recently have we been able to look at data matching in any significant way because of IT systems being better. That is primarily used now in terms of fraud, because what is very clear is that those who perpetrate benefit fraud are mainly two types. One is an individual who will just try to commit fraud but there are very organised large-scale frauds going on, and they tend to operate within regions over a large number of authorities. Up to now it has been quite difficult to catch them. You can obviously catch them within a local authority but data matching is helping that, and if you look at the Information Commissioner's advice, certainly he has covered quite clearly the issue about data matching, which I think covers that point satisfactorily.

Q888 ***Lord Peston:*** All of this was leading up to the point that we used the expression in our question whether local authorities receive sufficient guidance on this, but really we ought to be asking do individuals officials receive sufficient guidance? What is your view? If I can add another bit on that, one often refers to the need to know, but in a way, you do not know whether you need to know until you have tested it by getting the information in the first place.

Professor Morphet: Yes. There are two sorts of examples to think about. I have been primarily talking about benefit cases, where people have to divulge financial information. The training systems for that are very rigorous and they are inspected very closely. The need to know comes into play when you are doing casework around an individual, around a child, say, a child protection issue. There is quite a lot of distrust between organisations, in my experience anyway, at a formal level about sharing information. However, informally some of those conversations go on around a child because of concerns. When I was a chief executive, which is now ten years ago, we introduced social workers into secondary and primary schools because we had concerns. It is now becoming more common practice to have social work practitioners, certainly in large schools, and now associated with primary schools, and if that can go on, trust can be built and sharing information around the child is a more natural event. There are risks; on the other hand, the risks of not taking action are also very great, and I think that ability to take that judgement as a professional is something that is part of your daily tasks.

Q889 ***Lord Peston:*** Your view is it has to be done on an individual basis; in other words, if an authority were to say "Our principle in this authority is a presumption not to share" and another authority would take the view "Our presumption is you should share." That is your starting point. Where would you be on that?

Professor Morphet: I am talking now about individuals, who can have quite complicated lives. A child might live with its mother during the week and stay with its father in another authority at the weekend, and there might be concerns that need to be shared across the border. I would be on the side that, if there were concerns, they should be shared, but obviously in an appropriate manner. Depending on the scale of concern, I think it would be very important to do so, and particularly in urban areas, where local authority boundaries do not necessarily represent the patterns of movement and where people live, I think it is extraordinarily important that that is managed in a very proactive way, appropriately and to the case.

Q890 ***Lord Smith of Clifton:*** Might I ask: you were talking about contracting out to the Citizens Advice Bureau on Housing Benefit, and there are two things here. First of all, the Citizens Advice Bureau is taken generally to be advocates, yet they are exercising an agency function, so there is a real conflict of interest. Secondly, with contracting out to outside agencies, there must be a degree of control loss in terms of training. There are plenty of theoretical articles about the degree of control loss the more you contract out,

and there clearly needs to be rigorous training. I am sure it is on paper but who does the compliance on this?

Professor Morphet: On the point about the CAB, I take entirely the point that you make about a conflict of interests, but a number of agencies like the CAB now actually compete for this kind of work. There is a point of debate there, but that is the contract that we had.

Q891 ***Lord Smith of Clifton:*** Forgive me, you are just re-articulating the dilemma, not offering us any solutions.

Professor Morphet: I was just going to go on to say that thinking about the training side and how that is enforced, clearly, for many out-sourced contracts the actual out-sourced employees still sit within the local authority buildings and offices, so actually, the training and compliance happens in the same way as it would if they were in-house. Now each local authority has a risk and compliance officer as a requirement. Internal auditors also do systematic checks. DWP inspectors come on a regular and unannounced basis and, if there is any difficulty, they come back, having given you things to improve. Those agencies now use mystery shopping and other techniques to assess these things. They have IT compliance auditors as well, so now a local authority will have an IT compliance audit, which is precisely looking at the processes for handling data in terms of data quality, whether it is correct when it is inputted. We have all heard of people who have had problems because there have been mistakes. It also looks at the rigour of the internal systems and whether or not they can be breached by people from outside. I am not being glib about it. I think within a local authority it is such a systematic environment—and it is hard to convey that to you, I understand but that is the way it works. Perhaps it is hard to explain but it does happen every day.

Q892 ***Lord Smith of Clifton:*** I am happier with your answers on training but coming back to this conflict of interest by co-opting essentially the voluntary sector as agents of the state at a cheaper rate, and I think this is widespread, and not just the CAB and Housing Benefit, and so on, when we talk about citizens' trust in government, I must say if I thought in respect of my Housing Benefit they were not acting as advocates but were more concerned with renewing their contract with the local authority and did not want to cause too much trouble, this does not enhance my trust in the whole process.

Professor Morphet: I think that is a good point and I am not disagreeing with that at all. We did not have a contract with the CAB to actually issue Housing Benefit but they were giving housing advice on homelessness, finding people accommodation and that kind of advice. Nevertheless, even if you are establishing homelessness, you still have to establish the financial and personal circumstances of an individual. So I do understand the point that you are making and I do not know whether CAB still have that contract. This was ten years ago and the contract was extant between 1996 and 2000. Perhaps that has now changed.

Lord Smith of Clifton: I doubt it. Thank you.

Q893 ***Lord Morris of Aberavon:*** I think Lord Smith has covered largely what I wanted to ask. The CAB, for whose help I was very grateful as a constituency Member of Parliament, are a voluntary organisation. I am encouraged by what you say about training but how do you know that they train to the same standard as a local government employee?

Professor Morphet: Because they would be trained by the local authority or by the DWP in the same way, and their compliance would have to be subject to the same audit as the local authority. So if you have a contractor undertaking work for you, the local authority has the same obligations as if they had their own staff doing it. Those obligations do not reduce. So, in a sense, if a third party is doing the work for you, the obligation on you is greater to make sure the compliance is there.

Q894 ***Lord Lyell of Markyate:*** You were talking about multi-agency partnerships, and I was just trying to think of a circumstance. I am now going to mention a dodgy kind of character who may have more or less dodgy characters around him, probably less dodgy; somebody who is being chased by the child support agency, not paying their ex-wife, who may also possibly be applying for a waste disposal licence, or not applying for a waste disposal licence; may have come up on CCTV cameras as fly tipping; may be working on the black market, which is wife says he is doing to the CSA, whether he is or is not; may be claiming benefit or not, and the wife maybe claiming Housing Benefit, to which she may be entitled because she is being looked at. Those are about six different agencies. To what extent in practice are they actually sharing information today, in your knowledge?

Professor Morphet: If you look at that cluster of circumstances, which in some cases would not be unusual, what would happen is that you would probably look at each of those separately to see whether there was any link between them. So if there is an issue about income and means to pay, and that were related to a claim for, say, Housing Benefit on the part of the miscreant, if you like, I think that cluster of activities about means to pay and payment and the wife's circumstances would now be looked at together, or are more likely to be looked at together. If you look at fly tipping and applying for a licence,

those two things I think may be looked at together because you would want to check if somebody had been prosecuted for dumping before you issued a licence, no doubt. I am not an expert in that but I am assuming that is one of the checks that you might do. I think those two things come together. If somebody is turned up on CCTV, the only reason why, if they have been shown to be fly tipping, that is an issue for Trading Standards or Environmental Health or the police to take forward appropriately to prosecution if the evidence is there, and if the prosecution goes forward, that is no doubt taken into account when a licence is considered but I am afraid to say I do not know the formal position. What I am saying to you is I do not think those two sets of circumstances, which I have grouped into two, would necessarily be connected—only if the fly tipping or the waste management business was actually providing an income which the individual was citing as a means whereby they could or could not support the child.

Q895 ***Lord Lyell of Markyate:*** You are painting a picture which seems to be a fairly real one of somebody sitting behind a desk, scratching their head about one or two or possibly three of these issues, but in your experience, at the moment the computer from the CSA is not talking to the computer from the fly tipping cameras, et cetera, so that they all link together.
Professor Morphet: No, I have never seen any evidence of that kind and I could not see any justification for that at all. I could not see why anyone would do that at the moment, or in the future.

Q896 ***Lord Lyell of Markyate:*** But at the moment you do not think it is happening.
Professor Morphet: Certainly not, no.

Q897 ***Lord Rowlands:*** You may regret mentioning the CAB! In your local authority, if I were a resident, and I came in and said, "Look, I don't want my personal financial information to be handed over to a volunteer from the Citizens Advice Bureau (a) because I know him or her or (b) I expect my local authority to be my local authority", would I be prevented from receiving benefit if I refused consent in that case?
Professor Morphet: Certainly not. As I say, they were not providing actual casework on benefits. They were advising on homelessness.

Q898 ***Lord Rowlands:*** So the financial side was dealt with entirely by the local authority itself?
Professor Morphet: Yes. I am just saying that, in order to establish that you are homeless, you have to provide some information about yourself, which you might regard as information that you would want to keep secure. It could actually be information not so much about finance but about domestic violence, for example, and that would be the cause of homelessness, and that is something you would want to keep secure as well. There is always a backstop position, so that if you go into a local authority and you do not want to see the adviser who is allocated to you, you can request another one. The increase in local authority one-stop shops and multiple advisers trained provides a much better opportunity for individuals, a bit like going to a GP surgery; you have a choice but you can sometimes choose to go to one individual if you feel they know your case.

Q899 ***Lord Rowlands:*** Can I just widen the discussion? What we are beginning to find is, with the increasing ability to create bigger and bigger databases, the temptation and the ambition in some cases has been to try to profile people in a variety of ways, to see whether they are going to be more likely to be criminals or more likely to be at risk, et cetera. Have you come across this? What safeguards do you think are necessary to prevent this growing database and this greater profiling, which could end up in discrimination or could just be wrong information or out of date information? The bigger the database, the greater the risk.
Professor Morphet: I am not particularly aware of any profiling in use at the moment inside a local authority. I suspect what is more likely to happen is that the local authority would be undertaking risk assessments around certain types of individual or certain types of case. Thinking of an older person, the first time they have a fall is generally a trigger point to think that more problems are going to occur and therefore you might review the kind of support that you are giving to that individual. If you think about fraud, if somebody has been found frauding with one financial fraud, I think you would use that as a trigger point for an investigation to see if there are any other frauds, and that has always been the case actually. We might be better at it now because we have the data. I am still working inside local authorities, and I cannot think of any example of profiling that they might use, although now for large fraud cases in benefits that might be the case, a profile of certain circumstances would bring cases to attention for review. I think it would be triggered by the circumstances of the cases.

Q900 ***Lord Rowlands:*** This is very much in the air or is very much being promoted as a concept, the idea of using these databases to try and, as it were, forecast almost people's behaviour. If this goes on from your experience, what sort of safeguards should be built into it?
Professor Morphet: I think it rather depends on the purpose of its use. If you are looking at people at risk, by which I mean that certain families . . . I am

thinking of the case of one particular council in the Midlands that identified that certain families had a cluster of problems when they looked at issues, and compared some information across agencies. These families were clustered on an estate, and there were high levels of truancy, crime, debt, poor health and so on. They had at least some triggers to look at that and when they did, they found there was quite a strong clustering, and they have been in and targeted that area for a range of initiatives to improve the situation. From that point of view, it is justified, but I do not think you are talking about that. I think what you are talking about is profiling to identify people and pull them out. I think that is a much more difficult approach, unless you have at least two or three good indicators. For fraud I think it is more justified perhaps than anything else.

Q901 ***Lord Peston:*** Could you clarify something in your answers to Lord Lyell to some extent to me? Is it an absolute rule that, if data about an individual is to be shared, that individual is always told?
Professor Morphet: There are circumstances when you can share data without telling individuals, and that is when you have concerns about fraud. That has been the case for some time; that is not new. If you have established that somebody has been in a fraud situation, you can then search to see their other transactions with you to see if those have been fraudulent, and already local authorities are enabled to share that information with surrounding local authorities and indeed are asked about it.

Q902 ***Lord Peston:*** Is fraud the only example?
Professor Morphet: I think where a child or an individual is in danger is the other key area where you do not necessarily have to ask.

Q903 ***Lord Peston:*** The fact is, is it not, particularly if we have these multi-agency partnerships which Lord Lyell asked you about that I may not apply for a benefit or something that I am perfectly entitled to simply on the grounds that I do not want you to tell anybody else about it? Then what you will have done as a matter of social policy is stopped me having a benefit to which I am entitled because I also believe in my individual privacy. Is that not a very bad thing, no matter what you argue the positive side is? I as an individual am entitled to protection as an individual. Why is that not overwhelming? Take an example: I cannot walk even a yard without being in pain, therefore I have a blue badge; I meet every one of the criteria, but I might take a very dim view if anybody else was told that that was my condition. Equally, I might take a very dim view, since I cannot walk without pain, if I could not have a blue badge. I think my rights here are absolute. I would find it hard to put up a philosophical case even to do with fraud where you should be able to override my rights.
Professor Morphet: I think the kind of instance you cite, travelling on from the points I made, I do not think those points are connected. If you do not wish to apply for benefit or you do want do not want any information shared about any benefit information you have provided, financial data is not shared unless you explicitly agree to that. However, by the same token, if you look at fraud, Trading Standards will be another area where people behave fraudulently and you could share information between Trading Standards authorities, but I think you are looking at a proportionate risk there because with risk to the public, whether it is the public purse or the public as an individual, that is the line that is taken. That is not new legislation; that legislation has been in existence for many years to enable that to occur.

Q904 ***Lord Peston:*** The point I am trying to get over to you is that part of our inquiry is not whether it exists but whether it is getting worse, and the more I listen to our evidence, it seems to me it is getting a lot worse, that people are putting data together on broad grounds, which I can see the efficiency grounds for, yet I remain slightly unconvinced that the right to things like privacy in all this should not be overwhelming.
Professor Morphet: I do not think I would share that view. I think information can be brought together but under the very special circumstances that I have described. The other side is, say, for example, you are in receipt of Attendance Allowance, or you have applied for a free school meal, the question that is properly asked, if your financial circumstances are such that you have just become eligible for a free school meal, the approach would be "Would you like us to see based on your circumstances whether, firstly, you might be eligible for any other benefit?" but even then, at that point it can be the individual's responsibility to make those applications. Some authorities would say "Would you like us to prepare the forms for you based on the information and then you can sign them?" but I think at each stage there is a break point so the citizen is in charge of that. The only circumstances where really you would be looking at information is where there is a very considerable risk either around money or about people, so I do not think that has changed.

Q905 ***Lord Morris of Aberavon:*** Could I ask how Lord Peston's privacy is enshrined if he does not want information about his blue badge to be circulated in case he may be claiming Housing Benefit as well? Is it in a code of practice?
Professor Morphet: Any member of staff at a local authority who is entrusted with taking that information is covered by the same verification

framework that I was mentioning before, and the processes for taking that information, ensuring its quality, that it is actually correct, how it is used and how it is stored, is all subject to the same audit process that I described earlier.

Q906 ***Lord Morris of Aberavon:*** What is the audit process enshrined in?
Professor Morphet: It is enshrined in the DWP's verification framework and the audit process run by the Audit Commission.

Q907 ***Baroness Quin:*** I think my question has been largely eaten up, but there were a couple of things I would like to pick up on. In your answer to Lord Peston just a minute ago, would I be right in saying that actually the only occasions where data is shared without the subject's permission is when some criminal activity is suspected. Is that right?
Professor Morphet: Or where there is a suspected risk to, say, a child.

Q908 ***Baroness Quin:*** That would also probably be, if there was a risk involved, something that was against the law.
Professor Morphet: Yes.

Q909 ***Baroness Quin:*** Secondly, in the earlier answer you gave to our Chairman you said that you felt that the culture was against sharing of information between agencies. Am I right in thinking that, despite the Government's attempts over recent years to promote crime and disorder partnerships and inter-agency working, with laudable aims, actually, that has not been enough to overcome the cultural barrier to sharing of information?
Professor Morphet: That would be correct in my view. If you think about each government department that has responsibility appropriate to this area, they provide advice on information sharing directly to their own staff, so if you think about advice in terms of working with children, then DCSF will have advice, but I think from a local authority's point of view, it would be more helpful if that advice were enshrined in the code for the whole organisation. At the moment the advice, say, about children speaks from one government department, one set of officers or officials, so although if you look at the Information Commissioner's advice on a sharing code and you look at the advice from the DCSF, you probably would not see much difference if you were looking at a general level. For those who do not want to share information, they will pull out any nuance or phrase to argue sometimes, I am sad to say, that information cannot be shared. So I think there is quite a long way to go in changing the culture, as Lord Laming frequently points out. I do not think we have moved that far actually.

Q910 ***Lord Smith of Clifton:*** Professor Morphet, if you could now turn more to aspects of planning, on which you are an expert as well, has the planning profession formed a view that CCTV can play a positive role in the planning and design process for urban environments? Is there a search for less obtrusive ways of achieving safe and orderly public places?
Professor Morphet: I do not think the planning profession has ever particularly promoted CCTV. It has come from a range of sources, so obviously the public through their crime and disorder reduction partnerships and also colleagues in regeneration who want a secure environment for leisure or for retail environments in what might have been difficult town centres. Clearly, what we know is that CCTV does not seem to act as much of a deterrent, although it does help in catching perpetrators. From that point of view, planning has not particularly promoted CCTV. Planning has promoted good practice in safe and secure design. For example, I sit on the Olympic town planning committee and all the planning applications—not just because it is the Olympics; it would be the case elsewhere—go forward to the police for consideration on those issues, to make sure that a secure environment is being created. We try to ensure that the design is there at the outset, and we also ask specialists in particular cases to double-check that. I do not think the planning profession has been particularly promotive of that but it would be promotive of safe design.

Q911 ***Lord Smith of Clifton:*** It has learned from the walkways on various council estates and so on as a result of this.
Professor Morphet: Indeed, that is right.

Q912 ***Lord Smith of Clifton:*** The Olympic committee will not require you to run hell for leather in spiked shoes to avoid being mugged! You make this point that the extensive use of CCTV in public places is justified, even though there is little evidence of its effectiveness in crime reduction and public order. It seems to be a sort of comfort blanket.
Professor Morphet: I am sorry. I do not think I said it was justified. I said if you are asking where the push has come from, and yes, I think for some people it is seen as a comfort blanket, and they do feel more secure if they believe that if anything happens to them, the perpetrator could be caught, but I do not think anyone now particularly believes that CCTV acts as a deterrent.

Q913 ***Lord Rowlands:*** When we went to Canada and the United States, our interlocutors were bemused by the way in which in Britain CCTV cameras have been spawned in such numbers. They could not believe they would have got away with it in Canadian or

American society. Do you not think there is a need for a tighter process than this? Local authorities just do them off their own bat, do they not? They get a request or a demand, and up they go. We have had evidence saying the Information Commissioner should be involved. What do you think? You said planners are not involved. Do you think somebody should be more involved in this process?
Professor Morphet: Every time you place a camera there is an expectation that someone is looking at what is happening, and there is a cost involved, and I think it would be worthwhile to have a more strategic approach at, say, local authority level to how they are used and why, and the costs of managing them. Clearly, there may be cases where the police may have particular views in some circumstances about this, but I think it would be more worthwhile to have a more integrated approach to thinking about on-street safety, which would include design, CCTV, and the presence of police and other officials. I would certainly be in favour of local authority on-street inspectors who were looking at, say, parking or other enforcement activities on the street.

Q914 ***Lord Rowlands:*** Street lighting, for example, might be a better bet.
Professor Morphet: Indeed. I would be in favour of them perhaps being in uniform so that they demonstrated some kind of public presence for the local authority, and so that they would be ambassadors and people would feel more secure when they realised how many publicly paid employees there are on the streets. That could be done through a uniform or wearing a tabard for a street cleaner or an inspector. So there are ways in which that could be done which would give people more security. When I worked in Rutland, we had the highest fear of crime of any local authority area in the country as measured by Mori, but we also had the lowest incidence of crime. We did not have much CCTV either.

Q915 ***Lord Rowlands:*** I do not imagine Rutland as being a centre of crime.
Professor Morphet: Well, it was not. I think if people have no experience at all, their fear levels are much greater.

Q916 ***Lord Lyell of Markyate:*** A search for less obtrusive ways of achieving safe and orderly public places: you made the point about public officials wearing tabards. That seems very sensible. Many of us were brought up on a book called *The Territorial Imperative* and that spawned hundreds of closes with curtains twitching, and that is very effective, but can you give us a third example of good public space design?
Professor Morphet: If we are trying to encourage more people to walk and cycle to counter obesity and depression, clearly, footpaths and the way in which planting is used by the side of footpaths is very important, and the height of planting, because women feel unsafe walking by high planting, feeling that somebody could be lurking behind bushes and so on. That is just a question of management and maintenance and thinking about that. There is also an issue that if you can offset some of the planting away from the edge of the footpath, but as we are trying to promote this kind of activity, having safe design for anything for pedestrians or cyclists is important, and perhaps we have not thought about that enough.

Q917 ***Baroness Quin:*** In your experience, have local authorities ever reviewed the use of CCTV cameras in their areas and as a result removed or dismantled them?
Professor Morphet: I cannot give you any direct experience of that, no. I think it is all in the other direction. I will not say there are no authorities who have done that but none spring to mind, I am afraid.

Q918 ***Lord Morris of Aberavon:*** Professor, the use by local authorities of covert, targeted surveillance arises obviously from the Act, to detect crime or to prevent disorder. I want to ask you in particular about the decisions of senior local government officials and about the proportionality of the use of their powers. Where should the line be drawn? We have heard examples of the use of such machinery for the allocation of schools, which cannot in any event, in my view, be a question of proportionality. It is clearly outside the intention of the Act. Dustbins, whether they are over-full perhaps what they contain, is pushing it a bit in any event. What sort of training or guidance do local authorities officials have in taking decisions regarding covert, targeted surveillance?
Professor Morphet: There are some traditional areas where this has been used. Trading Standards, for example, would be a longstanding example of where officials are trained, for example, looking at market stalls, looking at dumping, looking at the way in which items are made or distributed, car repairs, and that kind of thing. I can think of covert operations, sending children into off-licences to buy alcohol or cigarettes. Some authorities do run covert operations of that kind. Those are more longstanding and I think have public acceptance. The ones that you have described in terms of schools and refuse are much more difficult to deal with. I do not think it needs covert surveillance. Having once been in charge of refuse collection, if I thought that we had a particular problem in a street or with a household, I would send an inspector along with the refuse collection team. I

do not think I would make that person covert. I would send them along each week or during the week as part of the normal inspection, because you have people out all the time. I do not think that has to be covert. If I have my staff in uniform, people can see them walking down the street, but I do think inspection is important if you have a persistent problem, because some persistent offenders in these areas can cause a lot of problems for their neighbours, and the authority gets the complaints, and people feel the authority is not doing its job if it is not dealing with that offender. Thinking about schools, I think this is a very emotive issue in communities. I do not think I myself would go down that line, although I can understand how exasperated some of my colleagues may feel about the extent people will go to to get their child into a particular school. What I would be doing is saying "What is wrong with the other schools?" and in terms of public policy, should we be improving the quality of all schools so that parents do not feel they just have to get their child into a particular school because it has the best key stage two results or whatever. So I would be looking at improving the rest, but what we have to recognise is that at local level this is the kind of issue that will absolutely fill the chief executive's postbag and that of the local members. I am not defending it because I think I would try other things but, nevertheless, I think locally the pressure in the local press and on councillors can be extraordinarily high over this kind of issue.

Q919 ***Lord Morris of Aberavon:*** I understand what you say when you say "I think I would try other things." I know as a former constituency MP for 40 years or more how emotive these matters can be so I am not quite innocent in this matter. Should the Act be used at all, is the point I made, for this purpose? An Act introduced to prevent or detect crime used for minor infractions, or maybe not infractions at all, of sending children to the wrong school, emotive or not, or lifting the dustbins or whatever, is not within the power of the Act at all. It is a nonsense.
Professor Morphet: As I say, I would be of the same view as you. I would be looking at proportionality there.

Q920 ***Lord Morris of Aberavon:*** I am sorry. It is not an issue of proportionality; it is not within the sphere of the Act.
Professor Morphet: I do not know the Act inside out to give an opinion on that but I generally support the line that you are taking.

Q921 ***Lord Rodgers of Quarry Bank:*** This is an easy one to finish, arising from one of your many roles in the 2012 Olympics, and maybe this is a rhetorical question: do you expect that the Games will make widespread use of advanced surveillance technologies for the purposes of crowd control, prevention of terrorism and law enforcement? Have there been any discussions with the Information Commissioner, and do you think what is happening at Beijing might be the model of what you would like to have in 2012?
Professor Morphet: I should say first of all I can only speak for the town planning part of the Olympic effort, because I do not sit on the main committee. We have certainly looked at crowd modelling and what would happen, clearly the design of escape routes and so on. Also, we are controlling a perimeter fence for the duration of the Games as part of the security process. We have also looked at the access into the site through railway lines and so on as part of the planning process but I am afraid to say I do not have any other knowledge around the use of technology in terms of who is going to buy tickets and how that will operate. We have certainly looked at security within the site as of part of the planning consideration.
Chairman: Professor Morphet, can I thank you very much for the evidence you have given. Thank you very much indeed.

WEDNESDAY 25 JUNE 2008

Present	Bledisloe, V	Quin, B
	Goodlad, L (Chairman)	Rodgers of Quarry Bank, L
	Morris of Aberavon, L	Rowlands, L
	O'Cathain, B	Smith of Clifton, L
	Norton of Louth, L	Woolf, L
	Peston, L	

Memorandum by the Ministry of Justice

INTRODUCTION

1. The Ministry of Justice (MOJ) is responsible for the Government's domestic policy on data protection and data sharing, and also represents the UK at European and International level.

2. There have been massive social and technological advancements in recent years which give citizens greater opportunities than they could have ever imagined. There is a need to gather and access personal information to: support the delivery of personalised and better public services; fight crime and protect public security; reduce the burden on business and the citizen, and tackle social exclusion through early intervention. This processing of personal information is demanded in greater quantity and in quicker time than ever before and this presents a variety of challenges to public service providers.

3. This Memorandum covers the issues relating to the collection and sharing of personal information and the safeguards provided by the Data Protection Act 1998 (DPA) and other legislation. It also covers the duties and powers of the Information Commissioner.

4. The Home Office has also contributed to this Memorandum in respect of its policies, which engage the legal framework that governs information sharing. The Home Office's evidence on these policies can be found at paragraphs 33 to 78.

THE LEGAL FRAMEWORK

5. The current legal framework around information sharing is in our view responsive and robust enough to meet both current and future needs. There is no single source of law that regulates the powers that a public body has to use and share personal information. The collection, use and disclosure of personal information are governed by a number of different areas of law. In domestic law, these include:

- the law that governs the actions of public bodies (administrative law);
- the Human Rights Act 1998 (HRA) and the European Convention on Human Rights (ECHR);
- the common law tort of breach of confidence; and
- the DPA

6. The DPA regulates the processing of personal data and processing includes collection, use, and distribution. It is underpinned by the framework of the ECHR, particularly the right to a private and family life under Article 8, which is now part of domestic law by virtue of the HRA. Neither the HRA nor the ECHR prevents the lawful and proportionate sharing of data. Confidentiality is also not an absolute bar to disclosure. At common law, or where there is a statutory discretion to disclose, it is possible to share confidential information where it is in the public interest to do so.

7. Statutory bodies have to rely on express or implied powers to share information while Ministers of the Crown may also be able to rely on common law or prerogative powers. However, where there is a relevant statutory provision occupying the same ground, this may operate so as to exclude these common law or prerogative powers.

8. Under the DPA, organisations and individuals must comply with the data protection principles in order to process personal data unless an exemption applies.[1] These principles include ensuring that data processing is fair and lawful, that data are processed only for specified and lawful purposes and that data are accurate.[2]

[1] DPA. s.4(4)
[2] DPA Sched 1, Pt 1, paras 1, 2 and 4.

Additionally the processing has to meet certain statutory conditions. In many of these conditions it is a requirement that processing be "necessary" for a particular function or purpose, eg for the performance of a contract or to protect the vital interests of the subject.[3]

9. Where sensitive personal data is involved, such as data related to political opinions or health, the processing must also meet a further set of conditions, eg that the processing is necessary for the administration of justice or for medical purposes.[4]

10. Under the DPA, the Information Commissioner is the UK's independent regulator.

The Role of the Commissioner

11. The Commissioner promotes compliance and good practice; manages the notification scheme and enforces the DPA and other legislation that he has powers to act upon.

12. The mechanisms which regulate and protect the use of personal information are always under review to ensure that they continue to protect the citizen and help achieve the balance between sharing and protecting. The MOJ and other Government Departments work closely with and consult the Commissioner's Office, and have due regard for his views when developing policy and legislative proposals.

13. The Commissioner has statutory powers to ensure compliance with the DPA. These enable him to serve enforcement, information and special information notices, and obtain warrants to enter premises to inspect, operate and test equipment used for processing personal information. He can also seize and inspect evidence of offences.

14. Under the DPA, the Commissioner presents Parliament with an Annual Report on the exercise of his functions under this Act. The powers of the Commissioner are kept under continuous review and the Government will consider legislative change where the case for additional regulatory control is established.

15. The Commissioner has other specific or general powers that he can use under other legislation. For example, in some circumstances he can use the stop now powers under the Enterprise Act 2002.

The Collection and Sharing of Personal Information

16. There is a general recognition across the public sector of the potential to deliver more efficient and effective public services, and bring benefits to society as a whole, through better use and sharing of information, within appropriate legal constraints. It is also becoming increasingly obvious that the challenges for information sharing in the future may well shift away from sharing within the public sector into a more complex environment of sharing between organisations that fall outside the traditional boundaries of the public sector but still deliver public functions.

17. Information sharing is already happening occurring to deliver personalised, better public services, fight crime and protect public security, reduce the burden on business and the citizen, and tackle social exclusion through early intervention.

18. Changes in technology are beginning to transform the public sector and enable better use of information. In the past, information was generally held on discrete databases or in paper files. These were effectively isolated from other sources of information, and had a limited capacity for storing data. New technologies, and the Internet in particular, now mean that databases hold more data and that it is easier than ever before to link information held in different databases and to transfer information from one place to another.

19. These advances in technology have been taken up by the private sector to change the way that commercial services are delivered. As a result, citizens also expect public services to be better tailored to their needs, more joined up, and for their personal information to be better protected. Innovations such as biometric passports; road congestion charging; and the development of the Police National Database have all been made possible by new technologies and are being used to collect a greater range and quantity of personal data than ever before. Proper use of these will build public confidence and security.

20. In Sir David Varney's report[5] on service transformation, he identified that citizens currently have to report a single change of circumstances to Government many times over. In one instance, bereavement, he identified some 44 different public sector agencies that had to be informed. Sir David Varney recommended the development of a service that would enable members of the public to report changes of circumstances—such as births, changes of address and bereavements—to Government just once.

[3] DPA, Sched 2.
[4] DPA, Sched 3.
[5] Sir David Varney's review into service transformation *Service Transformation: a Better Service for Citizens and Businesses, a Better Deal for Taxpayers.* See

21. This information would then be shared across Government securely. Individual projects using shared data are designed to ensure that they are secure—with security measures ranging from the design of the system; physical access and technological controls to training and security checks for staff access.

22. Responsible information sharing ensures that citizens have a say in how their personal information is shared among service providers. Efficient use of this information will avoid citizens having to give repeatedly the same information to a range of service providers.

23. Research[6] suggests that the public is willing to give out personal information to Government and allow it to be shared if there is a clear benefit to be gained by this information sharing. Improved services are seen as providing a clear benefit, but public concerns still remain about the way that information can and should be shared across Government, the wider public sector and with private organisations.

24. Society is rightly concerned that these new developments are being used appropriately and within a legal framework, with due regard for individual privacy and rights. The challenge is to achieve the balance between increased information sharing and protecting the privacy of the citizen from unnecessary intrusion.

25. The Government is therefore committed to ensuring that information sharing is undertaken in a transparent and controlled manner, with legal and process controls in place to ensure that information is not shared inappropriately or disproportionately. Once information has been collected, the Government is very careful in ensuring that sharing can only take place when it is not incompatible with the original purpose of collection an important protection in the DPA and the Directive which the DPA implements. The public needs to be satisfied that a proper balance is maintained between the benefits of sharing information and the right to privacy.

26. As a rule, the Government consults widely on its policy and legislative proposals, affording the public and key stakeholders the opportunity to voice their opinions and concerns in response. The Government also ensures that frontline practitioners and the public are aware of legislative effects through guidance, public awareness campaigns, and official website postings.

A Case by Case Approach

27. Sharing is not an end in itself. It is one of the foundations for improving services across the whole of the public sector and increasing public safety. Responsibility for developing and delivering individual policies across the whole spectrum of Government activity rests with lead departments. The Ministry has a central role in providing advice on policy and legislative proposals which engage on data protection and data sharing, and ensuring that all parts of Government apply the legal framework in a consistent manner.

28. The Government considers and introduces new data sharing provisions on a case-by-case basis. The data sharing arrangements, including safeguards to protect the privacy of individuals and their personal information, are designed specifically around the policy itself, taking into account technological and social issues relevant to that policy.

29. An example of this is the Digital Switchover (Disclosure of Information) Act 2007,[7] which received Royal Assent on 18 June 2007. The legislation allows the Department for Work and Pensions to pass the names and addresses of people eligible for financial help with the switch to digital television to the BBC (or a BBC controlled company). The measures are supported by organisations who represent vulnerable groups and we estimate 7m households will benefit from the digital help scheme. The Act also provides for custodial sentences for unlawful disclosure.

30. In July 2006, in response to concerns raised, the Secretary of State for the then Department for Constitutional Affairs (now the MOJ) made an Order under the DPA[8] to facilitate payment card issuers to process sensitive personal data (provided by law enforcement agencies) about customers who have received convictions or cautions for crimes relating to child abuse images, where their payment card was used to commit the offence.

31. This enables credit card companies to exercise their contractual rights and decide whether to close the account and/or remove the card. The MOJ consulted the Information Commissioner before making the order, as required by the DPA. In Parliamentary debate, the Government assured the House of Lords that the action was fair; balanced; the order was justified and that there would be no prejudice to the innocent party in the case of joint accounts.

[6] See *Public Services Policy Review; The Public View,* IPSOS MORI, 27 March 2007 http://www.ipsos-mori/citizensforum/finalreport.pdf
[7] Link to: The Digital Switchover (Disclosure of Information) Act 2007
[8] Link to: The Data Protection (Processing of Sensitive Personal Data) Order 2006

32. The Select Committee on the Merits of Statutory Instruments had described the Order as "a good example of an appropriate balance between the rights of the state and the rights of the individual".

33. Following the Commissioner's special report *What Price Privacy?*,[9] the Government is seeking to use the Criminal Justice and Immigration Bill, which was introduced in the House of Commons on 26 June, to amend the DPA to allow custodial sentences where access to personal information has been wilfully or deliberately misused.

Current Position on Surveillance Related Policies

Closed Circuit Television (CCTV)

34. There is a Code of Practice covering the users of CCTV. The code deals with surveillance in areas to which the public have largely free and unrestricted access. The Information Commissioner has a role in taking into account the extent to which users have complied with the CCTV Code of Practice when determining whether they have met their legal obligations on data protection.

35. Since February 2006, the Home Office, with the Association of Chief Police Officers (ACPO), has been conducting a review to develop a strategy for the future development of public space CCTV. The report of the review will be published shortly, together with proposals for implementing the strategy.

The National Identity Scheme

36. This scheme, which includes the introduction of identity cards, has been the subject of considerable public consultation and parliamentary scrutiny over the past five years. At every stage there has been a clear understanding of the need to balance the benefits from additional public protection with the need to safeguard civil liberties. Indeed the British Social Attitudes Survey, published in January 2007, found that 71% of those polled thought that the introduction of ID cards was a price worth paying to combat terrorism.

37. Public consultation started in July 2002 with publication of "Entitlement Cards and Identity Fraud" (Cm 5557) which included a chapter on data protection and privacy issues, including human rights. Draft legislation was also published for consultation in April 2004 (Cm 6178). Consultation involved reviewing comments from members of the public as well as from specialists such as the Information Commissioner; also during 2004 there was an inquiry by the Home Affairs Select Committee which took written and oral evidence from Ministers as well as external experts and interest groups.[10]

38. Interdepartmental consultations took place at official and ministerial level before the first Identity Cards Bill was introduced in 2004 (including preparation, though not for publication, of a formal ECHR memorandum on the Identity Cards Bill for the LP Cabinet committee).

39. A second Identity Cards Bill introduced in May 2005 became the Identity Cards Act 2006. During the passage of the Bill the then Home Secretary, Charles Clarke, wrote to the Joint Committee Human Rights (JCHR) setting out how the proposals were compatible with the HRA and with our obligations under the ECHR.

40. The Identity Cards Act 2006 establishes a new post of National Identity Scheme Commissioner who will make regular reports on the scheme's operation and the uses to which ID cards are put. The Commissioner's reports to the Home Secretary will be published and laid before Parliament.

National DNA Database (NDNAD)

41. *Human Rights:* The Criminal Justice and Police Act 2001 allows for the retention of all fingerprints and DNA samples taken on suspicion of involvement in a criminal offence. These may be used only for the purposes of prevention and detection of crime, the investigation of an offence or the conduct of a prosecution. The legislation has been challenged in the courts under the ECHR. On 12 September 2002 the legislation was ruled in the Court of Appeal not to have contravened the Convention.

42. ACPO and the Home Office have been looking at how the police can best use the opportunities provided by the Criminal Justice and Police Act 2001. A revision of the rules governing the weeding of records from the Police National Computer is being examined in parallel with consideration of the best way to retain data on

[9] Information Commissioner Special report to Parliament *What Price Privacy?* published in May 2006 www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf

[10] The Home Affairs Committee Report on Identity Cards was the fourth report, session 2003-2004 (HC 130) published on 30th July 2004. The Government response was published in October 2004 (Cm 6359)—see http://www.identitycards.gov.uk/downloads/id_response.pdf

fingerprints and DNA from individuals who have been acquitted. The Information Commissioner's Office is being fully consulted on this exercise.

43. The DNA profiles of individuals who have had samples taken lawfully under the Police and Criminal Evidence Act 1984, but against whom the prosecution was not proceeded with or who were subsequently acquitted by the courts, can be identified on the NDNAD. DNA samples are retained and used solely for the purposes of prevention and detection of crime; the investigation of an offence or the conduct of a prosecution and such use does not contravene data protection legislation.

44. Currently the fingerprints of persons who are acquitted or against whom charges have not been proceeded with are weeded from the National Automated Fingerprint Identification System (NAFIS) system. Once the acquittal/not proceeded with information is put on the Police National Computer a message is sent to NAFIS and the fingerprint record deleted. In light of the changes in the Criminal Justice and Police Act 2001, further proposals are under consideration in relation to the system to allow for the retention of fingerprints on NAFIS in such cases.

45. Existing safeguards for data use: Fundamentally the interests of law enforcement and data protection are identical in that information needs to be accurate, lawfully obtained, processed and protected securely. Safeguards are provided by the restrictions imposed by the Police and Criminal Evidence Act (PACE) and the DPA, and the oversight provided by the NDNAD Strategy Board and the Custodian. Further safeguards are to be provided by an Ethics Group to be responsible for reviewing the appropriateness of policy, decision making and practice.

Electronic Monitoring (EM)

46. EM is used predominantly to monitor a curfew condition imposed as a requirement of bail; a community sentence; a suspended custodial sentence or release on licence from prison. Contract staff responsible for the service are subject to Criminal Record Bureau (CRB) checks. EM schemes used for monitoring curfew conditions imposed by a court or Prison Governor derive from primary legislation.

47. Information on a subject's curfew record can be provided to the police or other agencies involved in the investigation or prevention of crime, in line with the requirements of the DPA. The release of such information must be approved by the Ministry of Justice unless the subject is a Multi-Agency Public Protection Arrangements (MAPPA), or Prolific or other Priority Offender (POPO), case.

48. In developing the policy and legislation a wide number of criminal justice stakeholders are involved in the consultation process, with human rights and data protection issues key considerations in the operation of the schemes. The Criminal Justice Act 2003 was preceded by two consultation documents, "Making Punishments Work" published in July 2001 and "Justice for All" in July 2002. The current contracts and protocols relating to electronic monitoring were developed to ensure that those subject to electronic tagging are treated decently, and subject only to the minimum personal intrusion required to manage their curfew.

Regulation of the Investigatory Powers Act 2000

49. The conduct by public authorities of what might be described as "traditional surveillance" which interferes with individuals' human right to respect for private and family life is permitted by the Intelligence Service Act 1994, Part III of the Police Act 1997 and Parts I and II of the Regulation of Investigatory Powers Act 2000 (RIPA).

50. Article 8 of the ECHR establishes both the right of individuals to have their privacy respected and that public authorities may interfere with that right where that is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or for the prevention of crime and disorder.

51. RIPA provides for the authorisation, in accordance with law, of necessary and proportionate conduct that will, or is likely to, interfere with an individual's rights and where private information about a person(s) is obtained. It is not legislation that authorises covert conduct. Rather, it authorises interference with individuals' rights.

52. RIPA and the 1994 and 1997 Acts are used by a wide range of public authorities—the security and intelligence agencies, the police service, local authorities and government departments and agencies—which have necessary and proportionate requirements to engage in conduct that can interfere with individuals' rights for legitimate purposes whether, for example, to safeguard national security or to prevent and detect crime.

53. Subject to various statutory safeguards and oversight, this conduct includes:

- interception of communications ("phone tapping")
- acquisition and disclosure of communications data (eg. details of telephone subscribers and their call records);
- covert observation and eavesdropping on conversations in private spaces, both premises or vehicles ("intrusive surveillance")
- covert observation and eavesdropping on conversations in public spaces and vehicle location tracking ("directed surveillance")
- covert entry on and interference with private property and interference with wireless telegraphy.

54. This conduct may be undertaken only when necessary for a legitimate aim and proportionate to that aim and is subject to strict independent oversight by the Chief Surveillance Commissioner, by the Interception of Communications Commissioner and the Intelligence Services Commissioner – all of whom report to the Prime Minister and to Parliament.

55. RIPA also provides access for complainants to an independent tribunal—the Investigatory Powers Tribunal, set up under RIPA to consider complaints and human rights claims arising from conduct involving regulated investigatory powers.

Criminal Records

56. The Criminal Records Bureau, established under Part V of the Police Act 1997, provides wider access to criminal record information through its Disclosure Service. It was launched on 11 March 2002. This service enables organisations in the public, private and voluntary sectors to make safer recruitment decisions by identifying candidates who may be unsuitable for certain work, especially that involve children or vulnerable adults.

57. A Home Office Circular 047/2003 made it clear that except where specific statutory provision is in place (including Part V of the Police Act 1997, under which the CRB operates), the governing principle must be that the police must safeguard sensitive personal information, and must not disclose such information to a third party unless there is good justification in the particular case.

58. The Police Information Access Panel (PIAP) chaired by ACPO now determines access to the Police National Computer (PNC). This group decides who will get access in the future, determined by business need in accordance with an Information Tribunal Judgement.[11]

59. ACPO also produced Retention Guidelines for Nominal Records on the Police National Computer. These guidelines became effective on 31 March 2006 and replaced the ACPO Weeding Rules. The Guidelines are based on the format of restricting access to PNC data rather than deletion of data.

60. Sir Rhys Davies QC was appointed in September 2003 as the Independent Monitor of local police information disclosed under the Criminal Records Bureau's Enhanced Disclosure process.[12] The Monitor's primary role is to review intelligence information released from local police records under sections 113B (4) and 113B (5) of the Police Act 1997, and, for the purposes of Article 8 of the ECHR, to ensure that the individuals' rights to a private life has not been infringed arbitrarily or unnecessarily.

Information Sharing Between Police Forces (IMPACT)

61. The IMPACT Programme is introducing new IT enabled business change that will ultimately deliver a national police database, which will provide a single source of operational information linking data currently held on local systems with that held on national systems such as the Police National Computer (PNC). It is also helping the Police Service to implement the requirements of the statutory Code of Practice on the Management of Police Information (MoPI) and the accompanying guidance.

62. Forces and other agencies remain under a strict duty to abide by the requirements of legislation and other regulations including on data protection, human rights, policing, criminal procedures, evidence and equality and diversity. The Programme is addressing these legal and policy issues in close partnership with the Police Service, the Home Office, the Ministry of Justice and the Information Commissioner. Regular contact with these stakeholders is maintained to obtain their views and to keep abreast of developments.

[11] The Information Tribunal Judgment of October 2005 in the case of the Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v The Information Commissioner made it clear that old information that would previously have been deleted could be retained by the police for policing purposes. However, such information could not be made available for other purposes.

[12] Work on his Third Report has just began (as at early July 2007)

63. Initial consultations have confirmed that there is nothing to preclude the widespread sharing of police information between policing agencies for policing purposes, and that this can be achieved by holding information on IT systems that other forces can access directly. The powers to share information are either vested in specific legislation or common law.

64. The Programme is now developing an Information Management and Assurance Policy that will consider in greater detail not just the minimum requirements of the regulatory framework, but also how the potential impact on individual privacy can be minimised (whilst recognising that some invasion of privacy is necessary in the wider public interest). Once agreed with key stakeholders it will be used to help shape the design and implementation of the national database, including the associated business change.

Data Sharing—Multi-agency

65. Multi-Agency Risk Assessment Conferences (MARACs) will provide a standardised approach to public protection for victims of domestic violence. A protocol for the information sharing process is in the final stages of reaching agreement with the Information Commissioner. Consideration is also being given to ways in which multi-agency risk assessment, information-sharing, management and interventions processes to prevent serious violence in circumstances where MAPPA and MARACs would not apply, could be improved. Any proposals which are developed will take full account of DPA and HRA legislation.

Fraud and the Serious Crime Bill

66. The Home Office has worked closely with Ministry of Justice officials and the Information Commissioner throughout the development of the policy on the Serious Crime Bill and its passage through Parliament.

67. Both the data sharing and data matching provisions of the Bill are premised on the basis that the processing of data under those clauses must comply with the DPA and the ECHR. The Bill also requires the Secretary of State to produce a code of practice to which public authorities sharing information through a specified anti-fraud organisation must adhere. The Secretary of State must consult the Information Commissioner and others when producing or altering the code.

68. The data matching provisions included from the outset a duty on the Audit Commission to produce a code of practice with respect to data matching exercises. The Audit Commission must consult the Information Commissioner and others when producing or altering the code.

Immigration

69. Border and immigration policy is developed, using standard best practice guidance, consulting and collaborating with partners, in a transparent and open way, based on the best possible analysis and use of evidence, and consistent with international obligations, data protection and human rights.

70. Policy proposals are scrutinised to ensure, among other things, that they comply with data protection and human rights legislation. The Ministry of Justice is also consulted as proposals are developed. Collective agreement from across Government is secured before policy is decided, or legislation introduced.

Examples

Simplification Project

71. A Simplification Project, seeking radically to simplify the legal framework of the Border and Immigration Agency, was launched on 6 June with an initial consultation paper. Subject to the Parliamentary timetable, the aim is to introduce comprehensive new primary legislation in 2008. The initial paper sets out principles for simplification and invites views, making clear the intention to consult extensively with staff, external stakeholders and the wider public in taking this work forward. Regulatory impact and equality impact assessments will be produced to support the later stages of the consultation process and compliance with data protection and human rights legislation will be ensured.

Enforcement Strategy

72. The enforcement strategy was required from the outset to be a cross-government strategy so engagement with other departments in the process of development was critical.

73. This engagement came in various forms:

- Early dialogue with key government departments and agencies to understand their issues and requirements for the strategy
- A series of collective seminars to drive a common understanding of the issues and a collective approach to finding solutions
- Focused bilateral negotiations to refine the terms of specific proposals involving other departments.
- Discussions were held in respect of specific issues relating to human rights and data protection with DCA (as was) and devolution (with Scotland Office)
- Collective agreement to the proposed strategy via the relevant cabinet committees (AMWG and AM).

74. In relation to human rights and data protection, the discussions centred on the potential breach of rules governing information sharing as an aid to enforcement. The strategy contains commitments to work within the legal framework.

75. The seminars with other departments focussed on the interactions between users (migrants) and service providers (government and intermediaries) to get a more refined understanding of:

- the type of interactions required to deliver the desired outcome
- the motivations and capacities that would shape those interactions
- the levers that exist to influence those motivations and capacities.

76. Engagement with a number of key stakeholders included the Association of Chief Police Officers, the Audit Commission, and the Confederation of British Industry, to test emerging analysis and proposals. A consultation event was held with a wider range of stakeholders to explore ideas.

77. To ensure that the strategy was grounded in analysis of the evidence, information was analysed from the following sources:

- operational data held by the Border and Immigration Agency
- relevant operational data held by other departments and agencies
- Home Office research
- wider academic research
- international experience using the FCO network.

Points Based System

78. The Border and Immigration Agency operates three taskforces which meet industry stakeholders from three key areas: General Employers, the Arts & Entertainment industry and members of the Education community. The representatives actively engage with the Agency to contribute to policy decisions and the implementation process. Engagement with other key stakeholders is equally maintained and includes the Immigration Law Practitioners Association, CBI and TUC.

79. Implementation of the Points Based System for Managed Migration followed an extensive public consultation exercise and the publication, in March 2006, of a Command Paper "A Points-Based System: Making Migration work for Britain". A key learning point for the transitional and implementation arrangements was issuing a Statement of Intent for each element of the system prior to launch; this will inform external stakeholders and the public and allow for an opportunity to raise potential problems. Ensuring consistency with human rights and data protection legislation are key considerations, likewise early engagement is made with the Department for Business, Enterprise and Regulatory Reform to ensure international commitments are not compromised.

July 2007

Additional memorandum by the Government

Introduction

1. This additional memorandum provides cross-governmental information on policies and practices on data sharing and collection. It covers the relevant work and information systems from the Departments for Business; Enterprise and Regulatory Reform; Her Majesty's Revenue and Customs; Communities and Local Government; the Government Fraud Review; Children, Schools and Families; Innovation, Universities and Skills; Health; Work and Pensions; and Transport for London. It also covers information on the work that has been undertaken in the data sharing and data protection area since the publication by the Government of its Information Sharing Vision Statement in September 2006.

Data Sharing Update

2. In September 2006, Government published its Information Sharing Vision Statement (the work of MISC 31, the Cabinet Committee on data sharing). This set out the Government's intention to improve public services, tackle crime and terrorism, and protect the vulnerable through increased public sector data sharing. It also reaffirmed the commitment to provide a robust framework for protecting the individual's rights to privacy.

3. Since then, Ministry of Justice (MoJ) has been undertaking work to inform the Service Transformation Agreement.

4. On 9 October 2007, the Government published its Service Transformation Agreement (STA), which will underpin the 30 Public Service Agreements (PSAs) which were announced as part of the Comprehensive Spending Review. The STA sets outs the Government's vision for the transformation of public services around the citizen and specific actions for individual Government departments.

5. As part of the Service Transformation Plans, the MoJ will lead a cross-government programme to deliver a package of measures over the next three to five years to overcome the current barriers to information sharing within the public sector. The aim of this programme is to "develop frameworks and mechanisms that enable public sector organisations to share information to improve personalised public services, increase public safety and tackle social exclusion in an environment of openness and respect for citizens' privacy and access rights".

6. On 25 October 2007 the Prime Minister asked the Information Commissioner, Richard Thomas, and Dr Mark Walport, Director of the Wellcome Trust, to undertake a review into how personal information is used and protected in both the private and public sectors. The review will consider whether there should be any changes to the way the Data Protection Act 1998 operates in the UK and the options for implementing any such changes. The recommendations will seek to take account of technological advances and strike a balance that ensures appropriate privacy and other safeguards for individuals and society, whilst enabling sharing information to protect the public, increasing transparency, enhancing public service delivery as well as the need to minimise the burden on business. The review report and recommendations will be submitted to the Secretary of State for Justice in the first half of 2008.

7. On 22 November 2007, following events at HMRC, the Prime Minister asked Kieran Poynter of PricewaterhouseCoopers to undertake a review into HMRC's data handling procedures. The interim report sets out the work Keiran Poynter has already put in hand and makes recommendations as to the immediate steps that HMRC must take to protect data security. HMRC has aready put in place a number of measures these include:

(a) the imposition of a complete ban on the transfer of bulk data without adequate security protection, such as encryption;

(b) measures to prevent the downloading of data without adequate security safeguards; and

(c) HMRC disabling all the personal and laptop computers it uses to prevent downloading of data on to removable media. These will only be reactivated with approval of a senior manager, and for a specific business-critical purpose.

8. A full report from Keiran Poynter is expected in Spring 2008.

9. The PM also announced that the Government would give the Information Commissioner the power to carry out spot-check inspections of Government Departments' compliance with the Data Protection Act 1998. These spot checks will start early in the New Year.

10. Also, the PM announced that Sir Gus O'Donnell would be undertaking a review to consider procedures in departments and agencies for the protection of personal data; consider their consistency with Government-wide policies and standards; consider the arrangements for ensuring that procedures are being fully and properly implemented and making recommendations on improvements. The first stage concluded on 10 December, involved Departments undertaking an analysis of their systems and procedure for complying with policies and standards on data protection, including making recommendations for practical improvements.

11. On 17 December the Sir Gus O'Donnell Review published Data Handling Procedures in Government: Interim Progress report which set out the findings of the review so far, an update of progress and detailed the next steps. In particular the next steps committed on extending the spots checks to the entire public sector and in principle to the introduction of new sanctions under the Data Protection Act for the most serious breaches of the principles. Both of these commitments will be consulted on early in 2008. Stage two of the Review will look collectively at improved standards and procedures across Whitehall. This is due to be completed in early 2008.

Evidence from Department for Business, Enterprise & Regulatory Reform (BERR)

Summary

1. The Department for Business, Enterprise & Regulatory Reform (BERR) is committed to fostering competitive markets in the UK, EU and worldwide. By fighting anti-competitive practices and promoting open markets, we enable companies to compete freely and fairly, giving UK consumers more choice and better value. To support this aim, BERR has an enforcement and regulatory capacity to investigate, prosecute and regulate a range of activities, including criminal offences relating to company and personal insolvency fraud and in relation to suspected fraud of health related compensation schemes for former employees of British Coal, who are now the responsibility of the Department; and the regulation of misconduct or unscrupulous practice in actively trading companies.

2. This response to the House of Lords Call for Evidence will only comment from the viewpoint of the regulatory and enforcement arm of BERR as described above. Any reference from this point onwards to "BERR" should be taken only to include these enforcement and regulatory arms of the Department. This response will examine the various ways in which BERR utilises private data, including that obtained by covert techniques, and assess the relative impact on the right to privacy of the individual and their corresponding relationship with the state, through their relationship with BERR. Further, although the Call for Evidence covers the wide topic of personal data issues, BERR's view will be restricted to the competencies of its enforcement and regulatory functions.

Data Collection

3. BERR has a need to access personal information to fight crime and protect both the consumer and the UK open market economy. Although some parts of BERR collect personal data to enable compensation claims to be assessed, in the main, BERR does not collect and hold personal and private information on citizens in the traditional sense, however generally gathers information to be used in an evidential format to found and support both civil and criminal actions. Thus, personal information is held for the length of time necessary to prove or disprove allegations and the concordant time after judicial process to facilitate any such appeals as may occur.

4. BERR obtains information under a variety of legislative permissions—the Data Protection Act 1998, the Anti-Terrorism, Crime & Security Act 2001, the Companies Act 1985 (although this relates to company material and not personal or private information), the Police and Criminal Evidence Act 1984 and the Regulation of Investigatory Powers Act 2000. In all of its dealings, BERR is subject to the checks of the Human Rights Act 1998, the European Convention on Human Rights and Fundamental Freedoms, the DPA 1998, PACE 1984 and the various auspices of administrative law governing public authorities.

5. Personal information which is required by BERR is requested with reference to the Data Protection Act 1998, if there is no more specific legal gateway in which information can be obtained. BERR uses the exemption at section 29 to request information (that might otherwise be withheld) for the explicit purpose of the prevention and detection of crime and the apprehension and prosecution of offenders, whilst section 35 is used where the information is required for the purpose of legal proceedings. The reasons for the request are outlined, giving the recipient of the request a choice whether to release the information or not, dependant on their opinion on the necessity of the information and whether they agree that the exemption applies to the request. A safeguard is inherent therefore in that information does not have to be provided unless the provider

feels that disclosure is justified and necessary to further the enquiry. It is submitted that any information gathered in such a way by BERR has therefore been impartially audited to protect privacy of citizens and minimise any risk of collateral intrusion.

6. The same audit process is conducted for any requests made under the Anti-Terrorism, Crime and Security Act 2001, section 19, again providing a level of assurance that the requested information is necessary, legally sought and for a specified, guaranteed purpose. Further, BERR guarantees that the information sought cannot be obtained by any other means, that it is of substantial value to the enquiry and that lack of the information would prejudice the enquiry. Again, these are safeguards used to protect the public from unnecessary intrusion into their private life and to ensure that BERR is complying with the requirements and ethos of the HRA and ECHR.

7. BERR is authorised under the Regulation of Investigatory Powers Act 2000 to conduct directed, non-intrusive surveillance, to authorise the conduct of covert human intelligence sources and to obtain communications data. BERR considers that these methods are fundamental, basic and crucial utensils of any investigative toolbox. During the period January 2006 to November 2007, BERR made six directed surveillance applications and four applications for the use of Covert Human Intelligence Sources ("CHIS"). During the same period, 68 notices to communication providers were issued, for communications data to be used in 17 enquiries. This may give the impression that BERR is not the most prolific user of RIPA. However, it is submitted that the potential to employ such a powerful tool is a basic requirement of investigation; effectively disarming BERR without the capacity. BERR places much emphasis on the criteria of proportionality and necessity, using the tool sparingly as a last resort after all other methods of obtaining the information have been exhausted. It can be argued that even if just one offender was brought to justice using information obtained under RIPA, the capacity would be justified. The information obtained is compelling, powerful and often irrefutable, for example in the case of company directors allegedly paying for goods from suppliers with stolen cheques. Communications data obtained regarding both telephone and Post Office box numbers proved links to the defendants, resulting in a guilty plea. Additionally, the example of the disqualified director running a haulage business, whereby telephone numbers on vehicles were demonstrated, through gathering communications data, to be diverted to the telephone number of the suspect assisted in bringing the offender to justice. The facility of RIPA results in fairer, swifter, more effective justice by proving or disproving allegations, reducing investigation times, obtaining guilty pleas where appropriate so freeing up court time and relieving witnesses of the trauma of having to give evidence.

8. BERR only interferes with the exercise of the right to respect for private and family life in accordance with the exemptions provided for in the ECHR, ie in accordance with the law of the HRA and RIPA. BERR is of the view that there will always have to be some sacrifice of personal privacy on the part of the individual in order to protect the welfare of society, citizens and the public purse and believes the public accept this trade-off. However, the sacrifice is only made in proportion with the seriousness of the allegation under investigation and if it is necessary as a line of enquiry of last resort. There is objective scrutiny by a Senior Investigating Officer impartial to the investigation, and in some cases impartial to the Unit undertaking the enquiry, before covert conduct is authorised. This accountability is provided for in RIPA and is further monitored by the Offices of the Surveillance and Interception Commissioners. It is submitted that there is little more that can be done to protect individual privacy from unnecessary intrusion whilst still affording a level of protection from fraud to the community at large. Removing this investigative tool would be tantamount to rendering BERR investigators ineffective, whilst allowing fraudsters to defraud with impunity. Further, it is suggested that any such action would be deeply unpopular with the general law abiding taxpayer who has a right to, and a legitimate expectation of, protection.

9. BERR also accesses private data by way of search warrants and orders for production of special procedure material under the Police and Criminal Evidence Act 1984, sections 8 and 9. Again, although the material obtained is often personal and private to the individual, the judicial scrutiny required before obtaining these orders and the inherent requirement of the court to construe and implement all decisions in line with the fundamental rights identified by European law and conventions provides independent analysis of BERR's requests to access personal information. The court adjudicates on the necessity and proportionality of any such request to protect the rights of the individual from unwarranted state intervention; thereby it is submitted, preserving their relationship of trust with the state.

10. It is submitted that it is the responsibility of each and every public authority to conduct any interaction with the public with legal care, consideration and a respect for fundamental human rights, particularly with regard to the collection, retention and sharing of personal data. The public judge the effectiveness, efficiency and integrity of the state on the basis of their dealings with public bodies. BERR takes the mantle and responsibility of public confidence very seriously, both understanding and acting to maintain the delicate

balance between individual liberties and the safeguarding of the community in a democratic society. BERR therefore feels that although the relationship between citizen and state is, of necessity, changing as society and crime is changing, it is still a relationship of trust and confidence.

Evidence from Her Majesty's Revenue and Customs (HMRC)

1. Her Majesty's Revenue and Customs (HMRC) is responsible for the collection and administration of Capital Gains Tax, Corporation Tax, Environmental Taxes, Income Tax, Inheritance Tax, National Insurance Contributions, Excise duties, Insurance Premium Tax, Petroleum Revenue Tax, Stamp Duty (including Land Tax and Reserve Tax) and VAT. HMRC also has functions in relation to Child Benefit, Child Trust Fund and Tax Credits, National Minimum Wage and the collection of student loans on behalf of the Department for Innovation, Universities and Skills. HMRC collects data in pursuit of all of these functions and this is held on secure databases.

2. A review is currently underway into security processes and procedures, as announced by the Chancellor on 20 November. The review which is being led by Kieran Poynter, Chairman of PricewaterhouseCoopers, will be looking at HMRC practices and procedures in the handling and transfer of confidential data. It will make recommendations on how internal processes can be strengthened and whether HMRC's wider processes for liaison with other organisations should be changed to reduce the risks. Details on these issues are not included in this report therefore, to avoid compromising the findings from this Review.

3. HMRC collects data in order to carry out its functions. The data ranges from tax information about the earnings of individuals, the turnover of businesses, data about employees and employers (tax codes, pay schemes etc), those entitled to tax credits and child benefit and child trust fund payments. Data is collected about transactions eg supplies of anything subject to tax including the sale of goods and services, the purchase of homes (stamp duty) and inheritance tax whilst HMRC's work at the frontier involves the collection and analysis of data about the import and export of goods, the movement of passengers and vehicles, suspected or proven smuggling activity and other relevant information.

4. In order to improve the extent to which individuals and businesses pay the right amount of tax due and receive the credits and payments to which they are entitled, and to reduce the compliance burden upon them, the data collected may be internally pooled where there is a legitimate need to do so and it is proportionate and appropriate.

5. HMRC conduct surveillance activity to obtain information in both civil and criminal investigation cases. Their directed and intrusive surveillance activity is conducted in accordance with the provisions of the Regulation of Investigatory Powers Act, the Police Act and the relevant codes of practice. The conduct of this surveillance activity is subject to scrutiny by the Interception of Communications Commissioner and the Surveillance Commissioner. All this surveillance activity is authorised in accordance with the codes of practice and, where appropriate by the relevant Commissioner and the Home Secretary.

6. HMRC aims to ensure that data is only used where lawful to do so and for the purposes for which it is intended. HMRC aims to balance the collection of data and use of surveillance activity with the need to protect privacy and maintain confidence that data will be used only where it is relevant, necessary and proportionate to do so and is adequately protected against misuse.

Evidence from Department of Communities and Local Government (CLG)

1. The Department of Communities and Local Government within its day-to-day operations may manage and hold personal information for various purposes. The most common form of personal information held is name and contact details on stakeholder consultation lists. For example the Gypsy and Traveller Stakeholders list is kept for the purpose of consultation and keeping our stakeholders informed and involved in our policy making processes. Such lists are maintained and updated by the policy officials in the relevant policy teams and are unlikely to be shared with officials across the department. Names are added and maintained on a stakeholder on request of the individual and consent can freely be withdrawn at any time.

2. It may be worth the committee noting, that although the department collects limited personal information in comparison to some other departments, we do provide guidance (where it has been identified as helpful or needed) to Local Authorities on the management and use of personal information which they control. For example the department is currently working on guidance for use and sharing of personal information for revenues and benefits departments within Local Authorities. Guidance is not legal advice but is designed to help Local Authorities determine the best position possible in respect to their particular circumstances and purposes.

3. Below are two examples of relevant work and information systems in CLG which the committee may find of interest.

Supporting People (SP)

4. SP was launched in 2003. It is a grant programme which enables the provision of housing support services to help vulnerable people maintain or improve their ability to live independently in their homes and their communities.

5. Providers complete a form recording standard information for each new service user they take on and send it to the Centre for Housing Research (CHR) in St Andrews University where the data collection, processing and preliminary statistical analysis is carried out. Summary statistics are sent to each Administering Authority and CLG on a quarterly basis and non-personal data is uploaded to a website hosted by St Andrews.

6. Additionally since 2007, providers complete a form for each service user who leaves their service (or on a sampling basis for clients in receipt of long-term services), which indicates how successful the service was in meeting the clients' needs (to assist them to achieve greater independent living). Forms are sent to St Andrews and are processed as above.

7. The personal information collected for this programme includes:

- Age (but not date of birth).
- Gender.
- Economic status.
- National Insurance number (optional and agreed by DWP, introduced at beginning of 2006–07).
- Ethnic origin (optional).
- Disability (optional on Outcomes form and will be introduced as an optional question on Client Records form for 2008–09).
- Which client group the client is defined by.
- Whether client has been accepted as requiring services under statutory frameworks.
- Whether client has been assessed as a higher risk.
- Whether client is subject to requirements under an ASBO.
- Source of referral.
- Type of referral (from within same authority or from another).
- Accommodation occupied prior to receiving support service.
- How long client has lived in authority where the service is being provided (if less than six months, where they lived before).
- Clients religion (optional and on Outcomes form only).
- How successful the support was in achieving a number of outcomes.

Benefits to the Citizen

8. Combining Client Record and Outcomes data allows analysis of patterns of clients moving through different services throughout England. Therefore, it provides a measure of progression which can:

- be used to assess clients' needs and so identify the level of need for services and in which areas;
- assist in the development of services—to ensure they are tailored to clients' needs;
- monitor performance of services—identifying where improvements can be made to services or the provision of services for clients;
- monitor effectiveness of the programme in delivering positive outcomes for individuals; and
- inform commissioning and contact management.

9. CLG ensures the following safeguards or methods of data management to ensure the sharing of personal information is kept to a minimum;

- National Insurance Numbers will not be linked to any database that would allow the identification of individual clients and National Insurance Numbers, and are not shared with anyone but CLG.

— CLG will not be able to identify any individuals from the national insurance number—the client's name and date of birth are not recorded.

— CLG owns the data and permission must be sought before disclosing it to any other organisation (as outlined in the terms of the contract with St Andrews).

Info4local Website

10. www.info4local.gov.uk is a one-stop web portal that gives local authorities and others quick and easy access to information from across central government. It is managed by a partnership of seven departments (Communities and Local Government, the Department for Children, Schools and Families, Defra, the Department for Transport, the Department for Work and Pensions and the Home Office). More than 70 departments, agencies and public bodies add information to info4local, including links to news, consultations, policy documents, guidance, circulars, newsletters, events, research, related links and more.

(a) Personal information collected for the programme includes:

11. An email alert service is sent twice a day to more than 53,000 subscribers. People can choose whether or not to subscribe to this free service. Subscribers fill in an online form in order to register and give the following information:[13]

— Full name.

— Email address.

— Password.

— Whether they work for a local authority and, if so, which one.

— Whether they work in central government, the voluntary and community sector, the NHS or other field. If so, they are asked which region they are based in.

12. They are asked to supply the following information:

— Job title.

— If they respond that the work in an "other" field, they are asked to specify which.

— Whether they wish to be included in future research.

All other parts of the form relate to information the subscriber would like to receive in their email alert.

13. We also have a contacts form. We ask people to include their telephone number if they want to discuss their query. The form asks for information, including the following:

— Full name.

— Email address.

— Area of work (central government, local government, local-government related organisation, NHS, voluntary and community sector, other): this is not a mandatory field.

14. We also collect information through customer satisfaction surveys and site usage information, using cookies, log files and page tagging techniques, including JavaScript.

Benefits to the Citizen

15. Subscribers to email alerts receive a service they have asked to receive and we need some personal information (eg email address) to deliver the service. Other information, such as details about their work, helps us to build up a picture of who is using info4local that we can use to target future promotion.

16. Customer satisfaction surveys are voluntary. They are a way of asking users' views about the service we provide and consulting them about future developments so that we can improve the service to them.

17. Site usage information also helps us to improve the service we provide. They show, for example, which information users have been most interested in.

[13] Not all of this information would constitute "personal data" under the Data Protection Act

Safeguards

18. CLG publish their privacy policy on info4local so that users understand the intended uses of any information that may be collected. CLG also has a commitment in place to communicate any changes to the privacy policy.

19. The information is stored on an externally hosted database server on DCLG's corporate hosting infrastructure. The only people who have access to the information as the site developers and authorised CLG personnel.

20. Access is restricted by user accounts so it is possible to trace back a change to a particular user account. In addition to the site developers' security credentials, CLG has also recently conducted a penetration test carried where we identified no outstanding vulnerabilities to be addressed.

Evidence from The Government Fraud Review (AG)

1. In 2006 a cross cutting interdepartmental group established by the Attorney General and the Chief Secretary conducted a Review of the way we combat fraud in England and Wales. It recommended a Government led, national anti fraud strategy to manage a holistic programme of shared knowledge, co-ordinated action and improved prevention across both the public and private sectors.

2. The damage caused to society and the economy is known to run into many billions of pounds annually. Fraud is known to fund and support most forms of organised crime and even terrorism. In addition, individual fraud victims suffer acute anxiety and stress and may lose confidence both in the security of financial services products and systems and in the Criminal Justice System itself.

3. Following extremely supportive public consultations, the key recommendations of the Fraud Review were accepted by the Government and will be implemented following funding being made available as part of the 2008–11 Comprehensive Spending Review. The principal architecture for the national strategy comprises a National Fraud Strategic Authority (NFSA), a National Lead Force for Fraud and a National Fraud Reporting and Intelligence Centre (NFRC).

4. These are being designed by joint public-private sector working groups and will be established serially during 2008–10. The working groups are under the direction of the Attorney General's Programme Board, which includes senior members of the Home Office, British Bankers' Association, the Association of Chief Police Officers Economic Crime Portfolio, Department of Work & Pensions, Association of British Insurers, Serious Fraud Office, Financial Services Authority, the Ministry of Justice and HM Revenue and Customs; and is chaired by the Director of Policy at the AG's Office.

5. The NFSA will provide the leadership for the National Strategy and will bring together all the key stakeholders (public and private), whose combined power and authority will ensure that co-ordinated action is taken to implement the agreed strategies.

6. Concerted action will be taken across the entire existing system, comprising deterrence, prevention, detection, investigation, law enforcement, sanctions and redress for victims. The Strategy will aim to protect public money, businesses and individual consumers from fraud and to increase the impact of joint anti fraud efforts and law enforcement.

7. Key to the success of the National Strategy will be the sharing of information and knowledge about fraud, enabling weaknesses to be addressed and anti fraud actions—be they preventive or deterrent—to have greater impact on fraud incidents and repeated offending. It is of fundamental importance to the success of the project that the rights of citizens be protected. Therefore, these information sharing arrangements must be compliant with both the Human Rights Act 1998 and Data Protection Act 1998 so that there is proper management, use and disclosure of the personal information in a manner which is necessary, reasonable and proportionate to achieve the intended aims of the national fraud strategy.

8. Existing sector strategies of this kind have already resulted in considerable success in reducing financial fraud in particular areas:

- The NHS counter fraud and security management service (CFSMS) achieved £189 million savings in 2005.
- The Audit Commission's National Fraud Initiative saved over £111 million in 2005–06.
- The DCPCU (Dedicated Cheque & Plastic Crime Unit, sponsored by APACS) saved £10 million.

9. Each 1% reduction in fraud losses in the Banking sector (which contributes some 8% of GDP annually) secures £2.8 million in extra Corporation tax. CIFAS (The UK fraud prevention service, operating in the financial sector) has estimated that more data sharing between the public and private sectors has the potential

to deliver between £137 million and £273 million annually in benefits to the public sector. The Serious Crime Act 2007 contains power for the Secretary of State to designate fraud prevention organisations for this purpose.

10. The NFSA will also have an important role in providing public information about fraud and in measuring and publicising the success of actions taken to prevent, deter and punish fraud offences. It will be able to build on lessons learned in frontline investigation and feed these into both policy making and the design of anti fraud systems. Businesses, Government Departments and individual potential victims will benefit from greater awareness of fraud losses and from the experiences of others in reducing these.

11. The NFRC will be a police led organisation, housed within the City of London Police; whose existing role as the lead force for fraud in London and the South East will be extended to provide the National Lead Force. The NFRC will contain a fraud intelligence analysis capability, to support the national anti fraud strategy, as well as providing an important service to the public in general and to fraud victims in particular. It will be essential to the success of the strategy to build knowledge and understanding of fraud methods, typologies and repeat offenders, so that vulnerabilities can be identified and addressed.conf

12. The NFRC is being designed in close co-operation with the Information Commissioner's Office. Its final form and processes have yet to be decided by the Programme Board; but its overriding object will be to manage the knowledge we have, and can obtain, about fraud; ie about those who commit frauds, their methods and their fields of operation, in order to maximise the impact of all anti fraud action across the entire law enforcement and crime prevention "system". One of the options for the NFRC's call centre functionality is a partnership with an existing government department call centre, such as the OFT's Scambusters network, the FSA's consumer hotline or those operated by DWP or HMRC.

13. The NFRC will eventually receive all reports of fraud offences or incidents, either directly from victims (individual or corporate) or in bulk from organisations that already record suspected or actual offences and incidents: the Police, SOCA, Government departments, specialist units such as CIFAS, the DCPCU and the Insurance Fraud Bureau, Regulators and their equivalents overseas. This will enable it to contribute important data for measuring fraud losses which will in turn direct a future risk based national strategic response to fraud. The analyses of fraud incidents performed by the NFRC will support and inform the NFSA's public awareness work and ensure a better service to all victims. A survey conducted during the Fraud Review indicated that fraud victims are anxious to ensure that others do not fall prey to the same frauds. The NFRC will have an important role to play in publicising fraud methods and informing the public of the specific weaknesses and vulnerabilities that fraud exploits.

14. Some of the technology to link the various databases may not yet exist; for example the Police National Database project; so it is likely that the NFRC's capability will be built in stages and that it will be the last building block supporting the National Strategy to become fully operational. The programme will be subject in due course to a Gateway Review conducted by the Office for Government Contracts.

15. The NFRC will analyse the reports of fraud received, adding intelligence received from police and other sources to provide packages for action by law enforcement, Regulators and the public and private sectors. It is anticipated that the organisation will benefit from secondments of experienced civilian staff from all these sectors, to ensure that appropriate packages are designed for maximum impact on fraud reduction.

16. The NFRC will adhere strictly to any Codes of Conduct produced by the Information Commissioner and/or the Ministry of Justice's Information Sharing Strategy projects. Its intelligence packages will be conforming to the National Intelligence Model (NIM).

Evidence from Department For Children, Schools And Families (DCFS) And The Department For Innovation, Universities And Skills (DIUS)

1. Effective sharing of data and information is central to the Department for Children, Schools and Families' (DCSF) ability to deliver better outcomes for children and learners. Better information sharing is crucial to safeguarding children and supporting the drive to personalise learning and to improve service delivery; it also contributes to improvements in efficiency and effectiveness, in reducing burdens on the front line, and in ensuring effective accountability. It is a cornerstone of the Every Child Matters (ECM) strategy to improve outcomes for all children and for delivery of many of our reform programmes such as specialised diplomas and vocational qualifications reform.

2. Better information sharing brings many benefits and the DCSF is determined to ensure that the benefits are balanced against the need for privacy and the safety and security of personal data and information. This is reflected in the design and delivery of programmes and the systems that support them. This includes

legislation when appropriate, guidance and training for practitioners, authorisation and authentication of users, and secure systems.

3. Much of DCSF activity depends on effective information sharing, both at the level of Government databases, and between individual practitioners. Every Child Matters is a cross-Government programme, led by DCSF, of system-wide reform of children's services that supports working across professional boundaries to co-ordinate services around the needs of individual children and young people. Similarly, the devolved nature of the education, skills and children's services sector, and large number of public bodies and institutions within it make effective sharing of data and information particularly important. This is increasingly the case as services are organised around the needs of customers.

4. Many of the major DCSF programmes depend on effective sharing of data, all of which aim to improve services to children, families and learners. Some are an essential force for protecting children and young people—ContactPoint and the Common Assessment Framework, and the new Vetting and Barring scheme, which is a cross-Departmental programme with the Home Office in the overall lead and DCSF and DH sharing the policy lead for children and for vulnerable adults respectively.

5. In July the Government announced that it will provide to front-line professionals in children's services support by implementing a single national IT system to support the Common Assessment Framework (eCAF).

6. The Common Assessment Framework (CAF) is a key element of the Every Child Matters programme to transform children's services by supporting more effective prevention and early intervention. Its goal is to provide a standardised approach for practitioners in the holistic assessment of a child's needs and the design of an integrated service to meet those needs.

7. eCAF will allow a practitioner to create electronically, store, and share a CAF securely. Completion of CAFs by different agencies and the subsequent exchanges of data between relevant agencies promote multi-agency working and early interventions. The complexities of cross border work are removed, as eCAF provides a consistent approach for all practitioners working in different agencies and locations, thus facilitating the effective and efficient delivery of a coordinated service. eCAF will only hold information about some (not all) children, with consent, and for a limited period of time.

8. Access to it will be granted only to authorised users who have undergone appropriate checks, including those provided by the Criminal Records Bureau. Practitioner use of the eCAF system will be audited to ensure information is only accessed where it is necessary for practitioners to do so, and so guard against inappropriate access by authorised users.

9. Sharing of data is central to the introduction of major reform programmes such as the Specialist Diplomas for 14 to 19 year olds. For example, this programme may result in a learner completing courses with a number of learning providers and qualification awarding bodies. Students may have a personal portfolio of evidence drawn from different sources. This portfolio (probably web based) would be portable and owned by the student. It would be capable of being updated from different sources (learning providers, employer assignments) and shared by the student with others including universities, colleges and employers. In this instance the sharing of data brings real benefits to the learner through greater transparency, choice and ownership and supports greater efficiency and effectiveness in the system.

10. We have recently led on work with partners across government, and more widely (including the Information Commissioner's Office (ICO)), to develop a practitioner guide on information sharing. The guidance is published as part of the Every Child Matters strategy and is proving a valuable tool for practitioners to enable them to know when and how they can share information legally and professionally, in compliance with the Data Protection Act, the Human Rights Act and the Common Law Duty of Confidentiality. It addresses sharing information as part of preventative services and enables practitioners to reach an informed and appropriate decision about whether information should be shared.

11. The Integrated Children's System (ICS) is a framework for working with children in need (as defined under the Children Act 1989) and their families. ICS provides a conceptual framework, a method of practice, and a business process to support practitioners and managers in undertaking the key tasks of assessment, planning, intervention and review, for looked after children and other children in need. It is based on an understanding of children's developmental needs in the context of parental capacity and wider family and environmental factors. It has full regard to current legislation. Because the work with children in need requires skilled use of detailed and complex information, ICS is designed to be supported by an electronic case record system.

12. A key aim of ICS is to provide frontline staff and their managers with the necessary help, through information communication technology (ICT), to record, collate, analyse and output the information required. There is no "ICS database". Each of the 150 top-tier local authorities has been required to adopt the

best practice principles enshrined in ICS, of assessment, planning, intervention and review. Authorities are required to ensure that the information needed for each of these key processes for responding to children in need in their own area is held electronically according to appropriate exemplars. This has meant that each authority has been developing it own existing IT systems to meet this challenge.

13. ICS users are not exempt from the legal requirements governing either the sharing of personal data or social care practice. The Children Act 1989 is clear that, whenever an assessment of a child's needs, either for services, accommodation, or protection, is made, the child's wishes and feelings must be taken into account.

14. The CCIS (Client Caseload Information System) is a well established operational system. It is currently managed by Connexions and is capable of monitoring the activities of young people at local authority and even ward level. CCIS was primarily designed as a tool for Connexions personal advisers and lead professionals to support effective intervention and identify the most vulnerable young people and their needs. It provides a framework for the consistent recording of information, which is used for performance management and measuring progress towards local targets for supporting those not in education, employment or training.

15. There are also programmes within the Department for Innovation, Universities and Skills (DIUS) which are about enabling efficiency, and improving educational attainment. The most notable is the Managing Information Across Partners (MIAP) programme will enable information about post-14 learners to be shared more efficiently between bodies such as schools, colleges and exam boards.

See Annex 2 for more details of MIAP.

16. The examples above demonstrate some of the benefits of data sharing to both the citizen and administrative systems. The DCSF aims to balance these benefits with the need to maintain privacy and security of data. We are very aware that if citizens are to take up the education, skills and children's services to which they are entitled they must have confidence in the way their personal data is handled and shared. While all services are subject to the appropriate legislation on privacy and security of data, we have also put in place a range of measures that aim to provide this confidence and accountability. This is achieved through a range of measures including appropriate legislation, guidance to practitioners, access control through authorisation and accreditation of practitioners and building security into system design.

17. Following the recent events in HMRC, DCSF undertook a review of its internal processes which is led by the Chief Information Officer reporting directly to the Permanent Secretary. We have also asked Deloitte to carry out an independent review of information security for ContactPoint, where we know people will want additional assurance.

18. We have strong arrangements in place to protect data held by the Department. The Departmental Security Unit has primacy on all security matters including IT security and Information Assurance, and reports directly to a Board member. Our Data Services Group leads on statistical returns and analysis and safeguards this material. Our Internal Audit Division is a major player in managing risk and ensuring compliance.

19. Data security is being built into the design and implementation of all the major DCSF programmes. A prime example is ContactPoint which will be the quick way for authorised professionals working with children to find out who else is working with the same child or young person, making it easier to deliver more coordinated support. This basic online directory will be available to authorised staff who need it to do their jobs. It is a key part of the Every Child Matters programme to improve outcomes for children.

20. The use of biometric systems can bring benefits to schools including reductions in bullying and better attendance, along with administrative efficiency and can have other advantages in this regard over other systems such as smart cards. The British Educational Communications and Technology Agency (Becta) is producing guidance on our behalf, and in consultation with the ICO, on the use of biometric systems in schools. This is in response to the growing numbers of schools that are using biometric systems to improve school management; mainly to register attendance, pay for meals or access the library. The guidance advises School governing bodies and headteachers (although parents and carers will also find the information useful) on the practical and legal steps they need to follow should they decide to introduce biometric systems. The guidance aims to ensure parents are fully informed about what the school is planning, that appropriate data security measures are in place and that parents and children have alternative access should that be necessary.

21. Becta has also published a technical specification for school infrastructure which sets out the security steps for ensuring that electronic data is kept secure, and safeguarded against a range of potential threats, including identity theft. These steps include establishing ICT security policies and procedures, and implementing appropriate physical security, data security, network security and Internet and remote access security.

22. ContactPoint will not hold assessments, record statements of need, academic performance, attendance, diet any subjective material or clinical observations about a child, nor will it hold opinions or views about a child's parents or carers. It will hold only the contact details of the child's carers, general practitioner surgery, school and other professionals working with the child. Authorised users will have to have had relevant training and to have undergone appropriate checks, including enhanced Criminal Records Bureau (CRB) certification and will be subject to the requirements of the new Vetting and Barring Scheme, established following the Bichard Inquiry to avoid harm, or risk of harm, to children and vulnerable adults.

See Annex 1 for more details of ContactPoint.

23. The National Pupil Database (NPD) is another example of the way in which data security is central to DCFS systems. The NPD has been recording information on pupils' attainment in education over a number of years. This information can be used effectively to see how pupils have progressed and whether particular initiatives—such as the Aim Higher programme, which aimed to increase participation in higher education—have had an impact.

24. Crucially, this information is held securely and researchers have to apply for access. Any data provided is anonymous: it shows comparative attainment levels, not the details of the pupils and can help researchers identify trends and evaluate policy initiatives.

25. Becta has worked closely with the Qualifications and Curriculum Authority (QCA) to ensure that the revised secondary curriculum includes references to the teaching of e-safety. This is reflected in the revised level descriptors for each of the key stages. Becta and the QCA have also developed an Internet Proficiency scheme for Key Stage 2 pupils.

26. The Child Exploitation and Online Protection Centre (CEOP) have also developed ThinkUKnow a primary and secondary education programme for schools which focuses on developing safe and responsible behaviours online. This has been delivered to over one million children.

27. Becta works closely with Local Authorities and schools to ensure that there are appropriate measures in place to cover education and training for teachers, leaders and pupils, a safe secure infrastructure, effective policies and monitoring procedures all underpinned by robust standards and frameworks.

28. Becta's approach to this issue has adopted two fundamental principles—protect children when in school and educate them for their lives outside of school. These principles have been supported in the four main areas of policy and practice, education and training, infrastructure and inspection and standards. In conjunction with the QCA, we have developed an Internet Proficiency scheme for Key Stage 2 pupils. We have evaluated safety products and built safety into our standards and frame-work contracts, most recently advising British Standards on a safety standard for home computers.

Vetting and Barring Scheme

29. The Vetting and Barring Scheme to be introduced under the Safeguarding Vulnerable Groups Act 2006 and following the Bichard Inquiry aims to help avoid harm, or risk of harm, to children and vulnerable adults. It aims to do this by preventing those who are deemed unsuitable to work with children and vulnerable adults from gaining access to them through their work. This will be done by:

- Providing employers with a more effective and streamlined vetting service for potential employees.
- Barring unsuitable individuals from working, or seeking to work, with children and vulnerable adults at the earliest opportunity.

30. The responsibility for taking barring decisions will lie with a new Independent Safeguarding Authority which will be an independent statutory body. The application processes for vetting and barring decisions will be run by the Criminal Records Bureau (CRB).

31. The Department takes issues around security and confidentiality of data very seriously. We want to ensure that it is only used for the purposes for which it is intended. Effective data sharing enables the delivery of better outcomes for children and learners, and helps to protect them from harm by preventing those who are barred from working with children having contact with them or data about them. The measures we are putting in place are designed to provide effective services while also addressing both the legislative requirements on privacy and security and building the confidence of citizens about the education, skills and children's services to which they are entitled.

Annex 1

ContactPoint

1. The purpose of ContactPoint is to support Children's Services Authorities and their partners in their duties to co-operate to promote the well-being of children, and to safeguard them and promote their welfare, as set down in Sections 10 and 11 of the Children Act 2004 and in the safeguarding duty on school and colleges in Section 175 of the Education Act 2002. The purpose of ContactPoint is not to support the fight against crime.

2. ContactPoint is being established under section 12 of the Children Act 2004. Regulations made under this section came into force on 1 August 2007.

3. The intention is that ContactPoint will be available in all Local Authority areas by the end of 2008. ContactPoint will be a basic online directory containing a record for each child up to the age of 18 in England. With their consent, the records of young people leaving care or with learning difficulties can be retained up to the age of 25. The record will contain basic demographic information about the child, details of the parent/carer(s) and the name and contact details of practitioners working with the child. It will not contain case information. The purpose of ContactPoint is to save time and support early intervention by allowing authorised practitioners to see who else is working with the same child.

4. ContactPoint will be populated with data from a range of existing national and local systems. Section 12 and the draft regulations set out what data is to be held and lists the persons and bodies who are permitted or required to supply this data. It is anticipated that these data sources will include case management systems used by Youth Offending Teams and in the future the e-Borders system currently being established by the Home Office.

5. ContactPoint will not be used to profile children or young people. No support for profiling is being designed into the system. Through extensive work with practitioners ContactPoint has been designed to help practitioners to find out who else is working with the same child or young person, making it easier to deliver more coordinated support.

6. Access to ContactPoint will be restricted to authorised staff who need it as part of their work. The regulations detail the categories of practitioner who are eligible to be granted access to ContactPoint, these include police officers, members of youth offending teams and staff at secure training centres. An individual will only be granted access if it is clear that they need access to support their work on safeguarding or improving wellbeing for children. It will not be acceptable for users to access the system to support enforcement activities. This will be made clear to all users through training and guidance (due to be issued in early 2008).

7. Before being granted access, individuals will also have to attend training and have received an enhanced disclosure from the Criminal Records Bureau (or equivalent vetting for police). All users will be authenticated to ContactPoint using strong (2-factor) authentication techniques in line with the e-Government Unit (eGU) guidance. Every access will be monitored and audited. Potential misuse will be subject to investigation and if necessary disciplinary and criminal proceedings.

8. There are no plans for data sharing between ContactPoint and the National Identity Register. The bulk disclosure of data from ContactPoint will only occur in anonymised or psuedonymised form. This is to support statistical analysis and for research purposes.

9. The regulations provide for the Secretary of State or a local authority to disclose information from ContactPoint where this is required by a court order or where this disclosure is necessary for the prevention or detection of crime of the prosecution of offenders. These provisions are intended only for limited circumstances are will be subject to a judgement on a case-by-case basis. As stated previously, ContactPoint is not intended to provide a tool for use in the fight against crime.

Annex 2

Managing Information Across Partners

1. Managing Information Across Partners (MIAP) arose from the post-16 reforms following the Learning and Skills Act 2000 and the legacy of disparate data policies and systems sector wide. There was a recognition that effective data management would help realise the benefits of the Government's reform agenda. MIAP now brings together over 40 post-14 learning and skills sector organisations who have signed up to a new framework for data sharing.

2. The MIAP service is very much in line with the Government's thinking around Information Sharing, and has been developed in full consultation with the Information Commissioner's Office (ICO). It is all about managing information sharing in a transparent and controlled way, with legal and process controls in place to ensure that information is shared appropriately. It is also about sharing information for the benefit of individuals whilst ensuring there are sufficient safeguards in place; with an appropriate balance being maintained between the need for appropriate sharing of information and the potential risks to privacy. Data Governance arrangements have been developed and published and are accessible on the MIAP website www.miap.gov.uk

3. The MIAP programme of improvement to data collection and sharing will be introduced over several years and will result in information being collected once, used many times and used by all organisations that are entitled to it. The MIAP service will remove bureaucracy for learners by making their interaction with the education and training sector easier; enabling them to access directly, for the first time, information held on them and to share that information with others so that they can receive a better service and/or confirm their qualification levels.

4. In practical terms MIAP is an internet based and technology enabled set of services, supported by common data definitions. It has three core parts:

— a *UK Register of Learning Providers*, launched in August 2005, where individuals and organisations can access information about individual learning providers (their contact details; their courses; and their performance) through a single route;

— from September 2007, MIAP has begun to assign Unique Learner Numbers (ULNs) to all individuals over the age of 14 undertaking publicly funded learning in schools and FE (and potentially HE). It will do this through the *Learner Registration Service (LRS)*. The service will hold the Unique Learner Number and enable other organisations to access the number and contain it in their systems, enabling third party to third party transactions about learners to be made much more easily;

— from September 2008, MIAP will enable individuals to access information held on them about their school and FE learning participation and achievement in the form of a *Learner Record*, which can be shared with frontline organisations and potential/existing employers as they wish. It is expected that other data sources will be added in due course, for example, more timely achievement information direct from awarding bodies, and HE information from universities. This system will also provide a data query service for registered users. The lifelong record of learning will be capable of editing by individuals who may not want to share all the details of their learning.

5. The Learner Registration Service and the Unique Learner Number support better processing of data. The Unique Learner Number will be held by both awarding bodies and learning providers making the transfer of data about enrolment on exams and achievement information more efficient and accurate. It will support the way that units of qualifications (being developed by the QCA through the Qualifications and Credit Framework and 14-19 Diplomas) can be brought together overtime at the individual level to confirm achievement towards full qualifications.

6. For Information Advice and Guidance and Learning Providers, including schools with post-14 pupils, MIAP offers operational benefits in communicating with other educational bodies, such as examinations boards, and will enable them to understand how their learners progress in future learning. The National Client Caseload Information System (NCCIS) will contain the Unique Learner Number and will be able to share the number with local Connexions systems, enabling transfer of information about individuals between schools/providers and Connexions to be much easier. This will facilitate better monitoring of local targets for supporting those not in employment, education or training.

7. MIAP is represented on the cross DCSF/DIUS Identity Management Stakeholder Group, which is looking at identity management across all ages in education. Work is ongoing to look at how MIAP can support that strategy.

8. It must be recognised that crime has become more sophisticated, complex and subsequently more difficult to prevent and detect, reflecting society's advances, changes in moral values and advances in technology. Citizenship and individualism in the 21st century is evolving with alacrity. As this individualism advances, it is submitted that interdependence between individuals and state actually increases, as traditional aspects and cohesiveness of society break down.[14] The measure of society is that criminal acts continue to offend deeply held aspects of the collective conscience and so increasingly citizens look to the state for protection; to enable crime to be prevented and detected under these conditions, the relationship between citizen and state cannot remain static. Some aspects of individual privacy must be sacrificed to protect the welfare and safety of society,

[14] Emile Durkheim (1859—1917)

citizens and the public purse and it is submitted that citizens respect and understand this. As long as the investigators of a democratic state continue to undertake their duties honestly, fairly, with integrity and in accordance with law, both domestic and European, public faith will be maintained.

Evidence from Department of Health (DH)

1. The Committee has requested written evidence from the Department of Health on surveillance and data collection activities and, in particular, the safeguards that are in place to protect privacy and the rights of the citizen.

2. The primary purpose for NHS data capture is to maintain a record of the care provided and the drugs prescribed by its staff. This informs subsequent care, provides an evidence base to resolve complaints and litigation, allows the quality of care provision to be monitored and supports a wide range of health service management activities including financial management, planning, research and epidemiology.

3. The NHS is currently in the midst of a major modernisation programme in respect of its information technology. It is moving away from organisational, or in many cases sub-organisational departmental records, which have been largely paper based, to a modern digital infrastructure. A core component of this programme is the development of the NHS Care Records Service (NHS CRS) which will, in due course, provide a nationally available, secure, lifelong patient record. Access to the NHS CRS is controlled via secure smartcard technology, available at the point of need by healthcare professionals who have a role based, legitimate relationship with the patient.

4. The NHS CRS will incorporate stringent security controls and safeguards to prevent unrestricted or uncontrolled access to personal information. Beyond that, patients will have the right, subject to rare public safety exceptions, to restrict access to their clinical information. The NHS CRS holds detailed clinical information locally, with a summary of key information held nationally so that it is available wherever and whenever it is needed. Citizens may choose not to have a national summary care record and can control how the information in their local detailed records is shared.

5. The Department of Health is a recipient of non-personal statistical data drawn from activity reports that are generated for management purposes within and across the NHS. The Health and Social Care Information Centre is the NHS body responsible for analysing NHS, and to a lesser extent, social care performance data. The Department also holds the contracts for the maintenance of a number of national databases which hold personal data, and which are accessed by NHS staff in the course of delivering, administering and planning care. These databases are only accessed centrally by Departmental staff to perform essential maintenance, resolve data quality issues or where required by law eg when a citizen asks to see what data is held.

6. An important additional component of the NHS IT modernisation programme is the creation of a Secondary Uses Service (SUS) which is used to generate anonymous or coded data to support management and research purposes—purposes usually described as "secondary" to the provision of care. This is an important new development in the context of safeguarding the personal data of citizens as it enables important activities to be supported without breaching privacy or confidentiality rules.

The overarching approach to privacy and safeguards

7. The NHS and the Department of Health treat patient privacy and confidentiality extremely seriously and there is a robust framework—usually referred to as information governance—which sets exacting standards and monitors organisational performance. This comprises:

- A National Information Governance Board, which advises Ministers on significant issues and monitors organisational performance. This board incorporates the statutory Patient Information Advisory Group that has provided a more limited leadership since 2001.
- Publication of a Care Records Guarantee that sets out the privacy and confidentiality commitments that the NHS makes to patients.
- Audits of information governance performance by the Healthcare Commission, the body responsible for assessing organisational compliance with key standards.
- Performance assessment of NHS organisations against detailed standards for legal compliance, security, data quality and records management set by the Department of Health in collaboration with key regulatory bodies, with performance data collected through an on line information governance toolkit.

— The appointment in each NHS body of a senior clinician, termed a Caldicott Guardian, who is responsible for championing patient confidentiality and advising management boards.

The NHS IT modernisation programme

8. The NHS IT Modernisation Programme has several components, a number of which are covered by the broad heading of the NHS Care Records Service:

— The Personal Demographics Service (PDS). This is a national register of all NHS patients. It does not contain clinical information, but holds the contact details, date of birth, unique NHS number and registered GP for each patient.

— The National Summary Care Record (SCR). This is a national database of key clinical information considered by clinicians as being important when providing care to a patient in the absence of full notes.

— Detailed Care Records. These are the digital replacements for traditional GP or hospital patient records, available across health communities and along care pathways. The SCR is derived from these records.

— The Secondary Uses Service (SUS). This is a database of clinical information that can be used to generate anonymised or pseudonymised (coded but not identifiable) data sets for research and management purposes.

There are a number of other components which modernise the services available for citizens which are not directly relevant to this Committee:

— Electronic Transfer of Prescriptions. This service supports paperless prescribing and collection of repeat prescriptions.

— Choose & Book. This service allows patients to be booked directly into clinics when referred by a GP, supporting choice and enabling appointments to be set around the requirements of citizens.

9. International security standards are applied across all system implementations. These include the use of encryption to communication links between systems, and to user interfaces with systems. The security of data centres is assured using both international and British standards, and all suppliers to the NHS IT Programme are contractually bound to auditing their adherence to these.

10. Users are vetted and sponsored by their local organisations for specific access appropriate to their job role and area of work. There is a strong registration process compliant with the highest government standard (eGif level 3) which means the user has to initially appear in person to prove their identity before access is assigned by the "Registration Authority" with accountability at local NHS Trust level. On successful completion of the registration process, a user is issued a smartcard—a secure token that, together with a passcode, confirms the identity of a user at the time of access. The registration process assigns them a role profile consistent with their area of work and responsibilities and establishes a unique electronic footprint when used to access systems. These records can be analysed to identify suspect behaviours.

11. There are a limited number of circumstances where systems may permit users with appropriate role profiles to access more data than their basic access privileges will permit. These circumstances are tightly defined and do not, for example, allow administrative staff to override controls in order to access clinical information. They include, for example, circumstances where a clinician is involved in the provision of emergency care and there is no time to establish appropriate access rights. When this occurs, the system generates an alert which is sent to designated privacy staff who will investigate to ensure there has been no misuse of the system.

Types of patient information collected, the options available to patients in respect of each, and the specific safeguards that apply

12. Patients' demographic details (name, address, NHS Number etc) are held nationally in the Personal Demographics Service (PDS), a key component of the NHS Care Records Service that is already in place and working well. These details are required to ensure that any previous records are located and that patients can be contacted when necessary. Regulations require the NHS to keep a record of which GP practice each person is registered with and reasons of efficiency and probity require this to be held centrally (eg to prevent multiple GPs from being paid for the same patient and to ensure that the correct commissioning body meets the cost of care provided). A register is also needed to enable the Secretary of State to meet legal obligations to provide healthcare, free at the point of contact, for those patients who are ordinarily resident in England.

13. Whilst NHS patients cannot exercise choice about their demographic data being held, they can ask for their contact details to be treated as sensitive. This prevents local NHS staff from seeing these details. This facility is used primarily to support those in witness protection programmes and military personnel, but is also available to anyone who is concerned about the ease with which NHS staff may be able to determine where they currently live eg people hiding from abusive partners.

14. Access to the Personal Demographics Service (PDS) by NHS staff is restricted to those issued with a smartcard and an appropriate role as described above. To locate a specific individual's records it is necessary for these staff to input sufficient information to obtain a unique match, generally only possible where the individual concerned is present and can be asked for details. If this proves difficult because there are too many individuals with similar details, a list can be accessed but doing so generates an alert to other staff responsible for ensuring and checking that the system is not being misused.

15. Clinicians are required by their professional regulator bodies to keep clear, accurate, legible and contemporaneous patient records which report the relevant clinical findings, the decisions made, the information given to patients, and any drugs or other treatment prescribed, and which serve to keep colleagues well informed when sharing the care of patients.

16. The NHS IT modernisation programme is replacing local stand alone systems or paper processes with modern digital systems that are integrated at a local level to support the care delivered by health communities. These new systems also enable key summary data to be extracted and held nationally to support care outside of the boundaries of the local health community and/or in unscheduled circumstances.

17. Only the duly authorised staff of organisations that are involved in providing care will have access to clinical information held within the NHS Care Records Service (NHS CRS). No system functionality will be available to an individual who does not possess a smartcard and know the associated pass code. The role profile that has been assigned to an individual through the registration process determines which system functions, and consequently which parts of a record, an individual who has logged on to the system can access.

18. A central record is also maintained within the systems of which patients each staff team—workgroup—are currently caring for. A GP Practice, an A&E Department or a clinic would be typical workgroups. This relationship, termed a "legitimate relationship" (LR) is a prerequisite of access to a specific patient's record. Without such a relationship access is prevented.

19. Full audit trails of who has done what, made possible by the unique identity associated with each smartcard, are maintained within systems and it is intended that these will be available to patients on request, as well as to staff charged with checking for system misuse by authorised staff. This is a considerable advance on what exists now with either paper or electronically held records.

20. These technical controls are complex to implement and there is a trade-off between usability and ease of access to data and questions relating to security and patient safety. The Department is therefore proceeding cautiously and consultatively to ensure that the right balance is struck.

21. Uniquely, the Department is also providing security controls that are set at the direction of patients. This provides unprecedented confidentiality management for patients of the NHS in England. Patients have a number of options. They were developed following extensive research and consultation with patients/carers/citizens and the NHS. Patients may choose—

(i) Not to have a national Summary Care Record by requesting this through the GP Practice where they are registered.

(ii) To direct that controls are set to prevent data sharing. In this case the SCR can only be viewed with the individual's express permission or in accordance with the exceptions to English common law confidentiality obligations. Local sharing of Detailed care records across organisational boundaries will also be prevented—essentially recreating the pre-NCRS situation.

22. In time, patients will also be able to designate some data items within a record as sensitive so that they cannot be viewed outside of the team that recorded the information without the individual's express permission, or where concerns are extreme, that they are not available at all outside of that team. These types of control are referred to as "sealed envelopes" and "sealed and locked envelopes" respectively.

Use of data held on the new systems for purposes other than the delivery of care eg clinical research

23. Exceptionally, disclosure of clinical information outside of a health context may be considered in cases of serious crime or where there are significant risks to other people, following the guidelines set out for the NHS in the Department of Health publication Confidentiality: NHS Code of Practice, a guidance document that was agreed with the Information Commissioner and the General Medical Council.

24. The primary purpose of the NHS Care Records Service (NHS CRS) is to support the delivery of care to patients. However, as a by-product of collecting information for operational patient care, the architecture of the NHS Care Records Service (NHS CRS) provides the opportunity to rationalise data abstraction, data flows, data management, analysis and reporting. This supports management and clinical purposes other than direct patient care, such as healthcare planning, commissioning, public health, clinical audit, benchmarking, performance improvement, research and clinical governance. The system by which this is done is called the Secondary Uses Service (SUS).

25. Wherever possible, data will extracted automatically as a by-product of NHS services supporting direct patient care, including the NHS Care Records Service (NHS CRS), Choose and Book and Electronic Transmission of Prescriptions. Initial Secondary Uses Service (SUS) content will cover the NHS in England and will be patient-specific. It will build on operational information already being shared by the NHS such as commissioning of healthcare services (eg diagnosis and procedures), cancer waiting times, clinical audit and supporting demographic data. Data will in due course cover all care settings (primary, community and acute) and all NHS-commissioned activity, including services provided for the NHS by the independent sector.

26. The aim is for this data to be made available either in aggregate form or, where detailed information is provided, in anonymised or pseudonymised form. This process removes patient identifiable information and allocates a consistent "pseudonym" so that individual cases can still be tracked, but only with explicit approval and still without identifying the individual concerned.

27. Access to identifiable information is available only where patient consent has been given, or where specific permissions apply. Permission is required from an expert group called the Patient Information Advisory Group (PIAG), set up under the Health and Social Care Act (2001). This group assesses each application to test that the use of patient information is justified, taking into account issues of confidentiality and consent.

28. As with all other elements of the NHS CRS, access to the Secondary Uses Service requires each user to be formally registered and to use individual smart card access, just as for other systems in the National Programme for IT in the NHS. Each user is allocated a role which determines the functions (ie what reports they can access) and the coverage (eg the organisation or geography of data which may be accessed). Key user activities, eg, logon and performing an extract, are logged.

Evidence from Department of Work and Pensions (DWP)

1. The Department for Work and Pensions (DWP) is here to promote opportunity and independence for all through modern, customer-focused services. We help people to achieve their potential through employment, so that they are able to provide for their children and to work and save for secure retirement. All this is part of building a fair and inclusive society. DWP's main customer groups are:

- children;
- people of working age;
- pensioners; and
- disabled people and their carers.

2. Just about everyone in Great Britain will deal with the Department or one of its eight businesses at some point in their lifetime.

3. Our business requires us to collect and hold a wide range of personal information. Sir David Varney's report for HM Treasury, Service transformation: A better service for citizens and businesses, a better deal for the taxpayer, published in December 2006, set out a vision for transforming the delivery of public services. It aims to make service delivery channels more responsive to the needs of citizens and business.

4. Our goal is to collect and use information effectively, efficiently and securely and in a way which enables the Department and wider government to fulfil its policy and delivery ambitions.

5. DWP holds personal information on all of its customers to enable it to carry out its business, gathered from customers, or from other government departments and public bodies:

- HM Revenue and Customs (HMRC);
- Department for Children, Schools and Families (DCSF);
- Department of Health;
- the Home Office (including the Immigration and Passport Service (IPS) and the Police);
- HM Court Service;

— NI Social Security Agency; and
— Local Authorities.

6. All data held by the Department is in accordance with relevant legislation including the Data Protection Act.

7. We hold basic identity details—name, address, date of birth etc—for all our customers, and bank account details if that is the customer's chosen method of payment. Other information held will depend on what benefits or services the Department provides for each customer.

8. Staff are provided with access to data in accordance with business requirements. All requests for access are approved by line management. Staff access to data is automatically audited by DWP systems, the audit logs produced are checked, on both a random basis and when particular conditions are satisfied. In addition staff accesses are randomly selected for management checking.

9. DWP shares information with other public bodies for a wide range of different purposes:

— to ensure customers receive their full entitlement, for example by identifying recipients of winter fuel payments and by identifying Housing Benefit and Council Tax Benefit customers who might also be entitled to Pensions Credit;
— to ensure our customers receive other help to which they are entitled, for example providing information to Local Authorities to verify entitlement to free school meals;
— to prevent and detect fraudulent claims, for example by matching death information from the General Register Office with our customer records; and
— to improve the services we deliver to customers, for example by using information to encourage customers to have their benefits paid into bank accounts.

10. DWP also carries out limited data matching with private sector sources, such as Credit Reference Agencies to help detect fraud. The Social Security Fraud Act provides a legal gateway where, under specified conditions, information can be requested from private sector organisations such as banks and building societies as part of gathering evidence in fraud investigations.

11. The Jobcentre Plus Fraud Investigation Service conducts criminal investigations for DWP into alleged benefit fraud. Investigations may involve the use of a number of techniques and access a range of data sources, guidance on the usage of which reflects relevant legislation and codes of practice. Surveillance can only be undertaken if it is necessary and proportionate to the alleged offence and has been properly authorised. This means that all other avenues must be considered first.

12. DWP's approach to data sharing is that new opportunities to improve public services are exploited, while ensuring information is shared legally and in line with public expectations. Joint approaches should be agreed across government and beyond and trusted standards and safeguards should be established and maintained.

13. DWP will only disclose personal data, or receive data from another organisation, where this is permitted in law, and where it complies with the Data Protection Act and Human Rights Act principles.

14. Data sharing is managed in DWP through the use of a simple Data Sharing Protocol, which sets out the information required to test the strategic fit and legality of proposals and ensures appropriate safeguards are in place.

15. The Protocol defines clear standards of behaviour; emphasises the need for a clear well defined case for data sharing; and stresses the need to undertake an assessment of the impact of any proposed data share.

Evidence from Transport for London (TfL)

1. As a major organisation and heavy user of over 10,000 CCTV cameras spread across its rail network, stations and roads in London and the fleet of 8,000 buses all equipped with CCTV cameras, Transport for London (TfL) welcomes the opportunity to submit written evidence to this inquiry.

2. TfL has a lawful obligation to provide a safe and efficient transport system in London and as such uses and maintains a number of data sources relating to the transport system to meet this obligation. TfL actively works with its stakeholders, passenger groups and the Information Commissioner to ensure that it holds, processes and discloses information in a transparent, proportionate, fair and lawful manner.

3. CCTV systems in particular are used successfully by TfL for both transport system management and delivering a safe and secure environment for those who travel on London's transport system. In addition to its own rail and bus networks, TfL has helped fund CCTV cameras on some National Rail stations and trains

serving London as well as paying the Metropolitan Police £60 million and British Transport Police £50 million for resources to provide a safe transport network. For example, we use on-bus CCTV to deal with crime and anti-social behaviour on buses and have worked in partnership with the Metropolitan Police to deal with individuals perpetrating crime on the bus network. This has led to over 1,000 convictions of individuals on the bus network and helped to deliver a more safe and secure environment for our passengers and staff.

4. In addition, the CCTV coverage of TfL's network proved invaluable to the police and Security Services in the aftermath of the incidents of 7 and 21 July 2005. It provided valuable intelligence to the Security Services and gave vital assistance in the investigation and prosecution of individuals involved in the incidents. The CCTV coverage of the network remains an essential component of protecting the system from terrorism and providing essential intelligence to the Police and security services to support this.

5. TfL also works with the police services in London in order to assist with the investigation of crime and disorder on and around the network and will, where it is lawful provide data to assist the police to investigate crime. There have been a number of recent high profile serious crimes that have been successfully solved with the assistance of data provided by TfL. There are clear procedures in place to govern the transfer of such data and ensure that any transfer is undertaken in a manner that is transparent, proportionate, fair and lawful.

6. TfL takes its responsibilities as the Data Controller of the personal data and CCTV images of our passengers very seriously and will not release data without careful consideration of the implications for Londoners. However, where the release can be undertaken in a transparent, proportionate, fair and lawful way and will benefit London—particularly by making a direct contribution to the safety and security of our passengers—we will work with partners to ensure that this is delivered effectively.

7. Our procedures are developed using legal advice, guidance from the Information Commissioner and our approach has been ratified by TfL Board. We continue to develop these procedures and protocols and they will be continually reviewed in line with case law, legal advice, and any updated guidance that is issued by the Information Commissioner. The bus operators who control in excess of 50,000 on-bus cameras have strict procedures that are agreed with TfL on handing the data and any disclosures made to the police and law enforcement agencies is done a transparent, proportionate, fair and lawful way. These procedures are regularly reviewed by TfL in line with our own. The operators receive regular visits to ensure compliance with these. We strive to balance the benefits we can deliver to our passengers with regard to safety, security, reliability and service responsiveness with the important privacy demands of our passengers.

8. In a TfL survey (carried out by MORI) of 1,003 respondents in December 2006, 87% of people said they supported increasing CCTV coverage and believe it will help to improve passenger safety on trains and in stations.

9. Overall, TfL believes that the use of CCTV data in a transparent, proportionate, fair and lawful manner allows us both to effectively protect our passengers and staff, and information about them, and provide a more safe, reliable and effective transport system for London.

January 2008

Examination of Witness

Witness: Mr Tony McNulty, a Member of the House of Commons, Minister for Security, Counter-terrorism, Crime and Policing, Home Office, examined.

Q922 ***Chairman:*** Good morning Minister. May I welcome you to the Committee; thank you very much indeed for joining us. We are being televised this morning so could I ask you please to identify yourself for the record.

Mr McNulty: Tony McNulty, Minister of State at the Home Office with responsibility for policing, crime, counter-terrorism and security.

Q923 ***Chairman:*** Minister, the Information Commissioner, as well as some others, has warned that the United Kingdom is "sleep walking into a surveillance society". Would you recognise such a thing as a surveillance society? Do you think that the Information Commissioner's warning is justified?

Mr McNulty: I think his warning is justified in the sense that there is a potential if we do not do things in the right fashion and regulate them appropriately that we may end up with something approaching a surveillance society. However, in the next breath I would say that I am not entirely sure what the Commissioner or anybody else means by a surveillance society. If they mean something approaching 1984 where every single element of what an individual does is regulated, surveyed and accounted for by some big brother state, then I do not think we are anywhere near that and I do not think we are sleepwalking towards it either. If they mean that generally as a society we are struggling with how to deal with the very positive benefits of new technology in all sorts of ways, the interface between

the individual and data both in the private and public sectors and how we wrestle with those issues, then I think it is a warning that we would do well to heed to prevent sleepwalking, which I do not think we are doing at the moment anyway. I hope that makes sense.

Q924 ***Chairman:*** Would you yourself define privacy wholly in terms of individual rights and values, set against the interests of society as a whole? Or would you recognise any social importance, on the other hand, in privacy in terms of its contribution to the democratic society in which people feel free to participate without the fear of being suspected or watched?
Mr McNulty: I think the warnings from some about a suspect society are all the more interesting and I think that is absolutely counter-intuitive to a democracy. As our democracy has developed we have struggled with the rights of the individual and privacy and that individual's responsibility, and the duty afforded to the state in terms of public protection and public welfare. It is always—I think it always has been—a balance and the debate we are having now is about striking that balance, given other factors like, as I say, technology data and all the other elements. I would, I think, as most people should, weigh in that balance very strongly the rights of the individual and those broader rights of the state. Where there is a contest, other than in extreme cases, the rights of the individual prevail rather than the state; that is our democratic tradition and value.

Q925 ***Lord Peston:*** I tend to bore all our witnesses by quoting John Stuart Mill's famous dictum and I will quote it again to you. He says that there is a circle around every individual human being which no government—be it that of the one of the few or the many—ought to be permitted to overstep, in other words there is this private area. When I put it to one of the regulators who was a judge and asked him whether that applied now—I think he was regulating phone tapping or something like that—he told me that that is dead. Parliament has passed a law that enables phone tapping and similar bugging to take place and therefore his view is merely to judge whether the case is appropriate. Do you have a view on that? Do you believe in the original 19th century view of one of the great English philosophers no matter what? You seem to be putting a trade off view.
Mr McNulty: I think it has always been about balance and I think John Stuart Mill was trying to strike the balance.

Q926 ***Lord Peston:*** No he was not; he categorically was not.
Mr McNulty: Let me finish. For him the balance then was that there was an absolute circle of privacy and space around the individual. I think that is still absolutely appropriate as an aspiration. My difficulty with that is that whatever the state does the use of technology, data and a whole host of other things will prevail anyway in the private sector. I am sure we will get onto CCTV but we think on estimate something like 80 per cent of the cameras are private so of course there needs to be a regulatory function for the state of what goes on in the private sector as well. I should think John Stuart Mill or anyone else will find it all the more difficult to function today, notwithstanding the state, in that absolute privacy circle, given what he wants to do with banks, buying houses and all sorts of other things. In that sense I do think things have moved on. Would I recast John Stuart Mill and come up with an equivalent sentiment for today given what I have said, I think I would and I think the starting principle must still be, as much as possible, to leave the individual citizen unfettered to go about their business.

Q927 ***Lord Peston:*** Are we to interpret what we are observing today as temporary, namely that there are some very special threats in our society at the moment—rather like things that were introduced in the war—or do you see what is happening is very much the now and there will not be a reversal?
Mr McNulty: Much of what is subject for debate today I think is today's normality. CCTV, DNA database and a whole range of these other elements are not there as a response to exceptional threats and exceptional circumstances. Clearly much of what we do specifically on counter-terror and other elements absolutely is; you are about to have the great fun of the debate we have just finished in terms of the Counter-Terrorism Bill to look at that exceptionalism. I do not think it would be fair to say that over recent times governments of either party have put CCTV in high streets or developed the DNA database purely as an exceptional measure for exceptional times; I think that is routine in the 21st century given all I have said about the utilisation of technology, data and everything else by the private and public sector.

Q928 ***Lord Peston:*** The other thing that those of us who are fairly ignorant learned about this, Minister, is the enormous technical advance that has occurred in the ability to engage in surveillance now. Essentially the worry one has is that if the technology exists why not use it? Do you have a role that says that it may exist but you should not use it?
Mr McNulty: We do and we equally have a role that asks if the technology is getting ahead of us so that whatever is today's highly developed technology is that still going to prevail for the very surveillance

purposes that the state requires it in terms of people's public safety? Is that going to be relevant in five or ten years' time? So we have both, keeping ahead of technological developments to say that it might be there but actually there is a wider good that says you should not use it. Equally, is today's technology going to still be available to protect us in five, ten, twenty years' time?

Q929 ***Lord Rodgers of Quarry Bank:*** Turning away from the very important philosophic questions as to your own role, I know we are told exactly what your particular roles are within the Department, but what is your relationship with the other major departments? Are you chairman of a cabinet committee with other members? We are going to see Michael Wills later, do you have a competitive attitude? I have a piece of paper from the news on Monday morning on the question of councils being told to stop using spy laws for trivial issues. That is not a statement from a department but nevertheless it is close to Government. Would you be involved? Would you react to that? Apart from seeing the press cuttings would you think it would affect your view? Ministers do not normally sit down just thinking; they are expected to act upon the consequences. I am not expecting you therefore to sit for a long time thinking about the nature of surveillance, but how does it work? I am asking about the system of government in that respect.
Mr McNulty: I will come back to that example, if I may, after a few opening remarks. It depends on the area. Meg Hillier in our Department is more readily the Home Office minister charged with cross-cutting use of information, databases and everything else. That happens to be her responsibility but I work very closely with her. She will sit alongside colleagues on the relevant cabinet committees looking at those wider issues. We cast our net wider but in terms of counter-terror we do have weekly meetings with a whole host of departments, including ministers, on a regular basis updating not simply the security position but also then taking some thematic conversations about matters such as this and broader from a range of departments. We are absolutely plugged in across Government in terms of the architecture and increasingly I think joined-up government is both a clumsy phrase and probably still an aspiration, but that is what we need regardless of politics in terms of addressing these issues and that is what we are trying to do. If we go back to Sir Simon Milton's letter as a particular example, I had already got in touch with John Healey (my equivalent in the Department for Communities and Local Government where local authorities sit) to say that we should meet the Surveillance Commissioner to discuss some aspects of how local authorities are using the RIPA legislation, so therefore reactive rather than just thinking about things. In the light of what Sir Simon Milton said I have written to Sir Simon to ask him to come in and talk to myself and to John Healey as well. I thought that was very useful on behalf of the Local Government Association. If you read his letter rather than just the headlines he was saying that these are important powers to deal with aspects of statute that local authorities are charged with control of and if there are abuses or misuses around the edges then that goes to the integrity of councils using these powers in the first place. It was not quite as sharp as some of the headlines were saying. That is exactly what I was thinking which is why I have asked John Healy to meet the commissioner and I have asked Sir Simon Milton to come in and see us too. If you read the RIPA legislation—the clue is in the title: Regulation of Investigatory Powers Act, not counter-terrorism but you can use it for the Litter Act as some would have it—of course terrorism and security was a key part of deliberations in both Houses but it was about some defence of the public from these powers invested in regulatory bodies, so we do react pro-actively (if that is an appropriate way of saying it) rather than simply sitting back and swerve the rigours on a daily basis and just carry on regardless.

Q930 ***Baroness Quin:*** Do you feel in joined-up government that there is enough focus on privacy issues in terms of the balance between those and security giving due weight to the privacy aspect? Are there discussions across Government on privacy?
Mr McNulty: There are discussions and the Prime Minister said last week that he is asking the commissioners in their turn to deal with the issue of privacy impact on the public and other matters in each of these areas. To go back to the original question, I do not accept the notion that we are sleepwalking into a surveillance society but I do accept that a lot of things are happening on a whole range of different fronts and it is difficult for any individual let alone the state to see what the cumulative impact of that is. I think both in his liberty speech some months ago and in the speech last week the Prime Minister was getting to a place to say "Let's have a look at the totality now of what prevails". I remember once arguing with him when we had the ID cards debate and trying to picture a normal day in an individual's life and the interactions they had with all sorts of databases, technology and potential surveillance or audit trails of their activities. You can cover most of the day and not even mention the state. I do think we need to look at that broader impact a bit more readily.

Q931 ***Lord Rowlands:*** Minister, we have heard from a variety of witnesses who have expressed deep concern at the way in which we legislate on the issue,

that powers to collect and share personal data are reserved more for secondary legislation than primary legislation and, as a result, we have seen a kind of creep—a very considerable creep—an expansion by stealth, as it were, of both collecting and sharing data that a member of either House could not have spotted in the primary legislation. We have been provided with an example by Dr Chris Pounder in his detailed written evidence on the ID Card Act where he illustrates that point, the Children Act 2004 and the Anti-Terrorism, Crime and Security Act 2001. The National Pupil Database started off quite innocently in 1997 and again it has grown and grown and grown. First of all, how do you do that? Secondly is it not time that we had a kind of parliamentary view of privacy impact assessments on bills and legislation?
Mr McNulty: On that latter point I think that is very, very interesting and one on which there should be further debate. Quite what a privacy impact assessment would look like compared to some of the other impacts would be very, very interesting and I would not decry a move in that direction at all. On the broader point I think actually the person who prayed in aid the ID Card Bill was fundamentally wrong on the level of some notion of data creep or function creep because everything available to Government in terms of ID cards was quite properly put on the face of the Bill and any changes to that have to come back to the House and there are a whole series of reasons in the Bill that go to the raison d'être for the register that they have to pass before they even go into orders. He is right, if I may say so, on the fact that the ID cards have increasingly more pieces of legislation; I quoted the other day 71 and was corrected to say that it was 74 order making powers springing from the ID Card Bill, but he is wrong in the essence of that meaning function creep in terms of the data. The data is very, very explicit on the face of the Bill or in schedule one. The issue is about whether it is appropriate for bills to more and more readily look like Christmas trees with all sorts of order making powers and, if you are interested, I am having a hard time following when that order is going to come subsequently because there are invariably delays to these things. That is a moot point and one that we should look at. The more serious matter is the principles that at least should be on the face of a bill. However, I have done enough bills to know that if you go in for undue specificity in terms of expressing things on the face of the bill, you sometimes cause more problems than leaving things more general. In the Counter-Terrorism Bill that you are about to inherit I think we have been as parsimonious as we can be on order making powers, save for the sort of 42 day model but I do not want to go down there necessarily today unless your Lordships want to. I do accept the premise that at least very, very clearly the principle and as much as possible the explicit functions and criteria for any data should be on the face of a bill as much as possible.

Q932 ***Lord Rowlands:*** In the case of Dr Pounder's evidence, will you give us a written comment on it.
Mr McNulty: I will.

Q933 ***Lord Rowlands:*** On the broader question I would like to pursue this question of a kind of privacy impact assessment on legislation and to say that some minister bringing forward a bill would have to make it very explicit as to what kind of information is being sought and what is going to be shared as a consequence of the legislation. Would you accept that alongside the human rights issue?
Mr McNulty: I think we are almost half way there in the sense that any new legislation to do with surveillance information or data will invariably have the comments of the relevant commissioner as part of the process.

Q934 ***Lord Rowlands:*** I have not seen any explanatory memoranda.
Mr McNulty: Not necessarily in the explanatory memoranda or as part of the official documentation, but fairly soon after the publication of the Bill you will have the views of the commissioner forthcoming whether requested or otherwise. That is perfectly fair because that is their role. I am not offering that instead of privacy impact assessments, especially in areas of real sensitivity. As I say, I think it is a point worth exploring. I am trying to think through the practicalities of what it would look like rather than dismissing the notion. I think it is a fair point.

Q935 ***Lord Rowlands:*** You mentioned earlier that technical innovation almost outstrips legislation and even decision making and ministerial accountability. Is there any way we could have a parliamentary process where renewal of a power would be needed when technology has actually changed sufficiently to create a much bigger problem for the privacy of an individual?
Mr McNulty: I think if there is substantive change it should come back in some form or other, whether it is an information point or for renewal. You will know that the Leader of the House of Commons is looking at the notion of almost annual, if not bi-annual, reports back on legislation to see whether it was implemented, whether it was all utilised.

Q936 ***Lord Rowlands:*** Post-legislative scrutiny.
Mr McNulty: Post-scrutiny, absolutely, and I think that might be the appropriate way forward for newer legislation but I do take the implicit point you make about a whole host of legislation now that was at least at its statutory root developed in an entirely different time in terms of technology; that might be fair. To

give you an example, the Police and Criminal Evidence Act has stood up extraordinarily well with tweaks along the way. We have just done a review on it and the most remarkable thing about the review is how comfortable people are on a consensual basis with the essence of it. If you look at it utterly literally—I have seen the outcome of this—it says there should be tape recordings of interviews and they should be portable. Every time I go to police stations I see cupboards stacked with cassettes, sometimes changed a little bit in terms of smaller digitals. We have requested permission under an order to conduct an experiment in the East Lancs Division of Lancashire Constabulary to do it on a digital recording basis with encrypted and sole access by the police and the defendant's side who require it so it is absolutely secure so nobody is lugging around cartloads of taped interviews. That technology was not anticipated in 1984.

Q937 ***Lord Rowlands:*** Would that require a change in legislation?
Mr McNulty: I think we can implement that universally on a wider order. We certainly have to bring an order to both Houses to even go down that route as an experiment. Perhaps I am proving your case rather than otherwise by saying that we can probably do that through secondary legislation. There has been a good deal of tweaking and changes to PACE by secondary legislation, broadly with agreement that it has been improved rather than otherwise, which is why the overall statutory roots have stood the test of time.

Q938 ***Lord Morris of Aberavon:*** Minister, I am encouraged by your pro-active role following the Milton letter, but the Home Office must have known for a long time that there were a lot of controversial decisions by local government long before the Milton letter which may well be the basis for his concern. We have heard cases, we have cross-examined witnesses from dustbins to school catchment areas so this has been well-known, in the press for a very long time of local authorities apparently exceeding what might be regarded as a proportionate action to RIPA. Had that not occurred to the Home Office before? Secondly, I think Charles Clarke was in your seat when he sent a letter when RIPA was being taken through the House to Bill Cash. I do not have it with me today but we can get a copy for you. He gave a categorical assurance that RIPA would not apply to local government. Should these powers be given to local government, whatever the basis of them?
Mr McNulty: As I say, if we afford a whole host of statutory powers to local government and expect them to enact those powers, then if they feel they need the sort of powers referred to in RIPA then that is entirely a matter for them, so long as they are used on a proportionate and rational basis. The key word you latched upon in your description was "apparently" because I do not have hard evidence that there are local councils up and down the country routinely misusing, abusing or wrongly utilising RIPA. I have significant anecdotal evidence—if I can say it in those terms, certainly not substantive empirical evidence—from some of the newspapers that it has been used disproportionately which I think may well be the case in one or two of the dog fouling, schools and other cases. If we are seriously asking local government to carry out its statutory functions around a whole host of things like the dispersement of assorted benefits, like environmental health, fly tipping and a whole host of others, and to challenge serious criminal activities that matter to their communities, we need to give them the powers to do that. I do accept that there is sufficient disquiet, not least from Sir Simon's letter, that goes to the integrity of local government using those powers at all, and that cannot be right which is why I am very keen to meet him with John Healy and why I had already set in train a meeting with the Surveillance Commissioner to discuss it with him. It would be unfair of me to say at this stage that there has been utter and broad misuse.

Q939 ***Lord Morris of Aberavon:*** There have been cases at the edge.
Mr McNulty: At the edge may be a fair description and I think we need to look at that in more substance.

Q940 ***Lord Morris of Aberavon:*** It may be the reason why Charles Clarke sent a letter in 2001 and the order was introduced contrary to his promise in 2003.
Mr McNulty: I could not possibly comment on that. Certainly looking from 2008 and what I know of RIPA I find it astonishing that anyone would say of all the public authorities local government probably would not have scope to utilise this.

Q941 ***Lord Morris of Aberavon:*** We will get the letter for you.
Mr McNulty: Thank you.

Q942 ***Lord Morris of Aberavon:*** Could I ask you about the tests of necessity and proportionality which officials at whatever level have to reach in the sense of whether it is appropriate to use powers in data collection and surveillance when there is a lack of benchmarks on how specific proposals could be judged? Have you thought about that?
Mr McNulty: We have in a very general sense. Clearly the more sensitive and the more intrusive the surveillance the more at the centre we are very, very clear about what those edges—as you referred to—are and what is permissible or otherwise. That is why it still remains the case that warranty is signed at secretary of state level for those very, very intrusive

but necessary interventions. I think the discussion about Sir Simon and local government goes to the broader issue about those thought processes and, as you say, we are not anticipating either function creep or power creep, if that is appropriate and people pushing at those edges. To go back to one of my earlier answers, I think that is done fairly rigorously in its own terms within a bill but I am not sure if sufficient is done to put that bill in the context of what is already out there, rather like the broader point about privacy and impacts and how this one additional element adds to the greater cumulative lot that is out there. I thought it was interesting—and I tease my officials about this—that at the end of the supposed questions that were coming my way it said, "What, in your view, are the four processes through which officials ought to go?" I could do a lecture on that in the broader general sense but not specific to these issues. Officials do consider proportionality and matters like that. I think collectively Government might have to learn a lesson about how to that more readily across the piece. That is almost the same point I was making about joined-up government.

Q943 ***Lord Morris of Aberavon:*** Proportionality is not always an easy decision and given the lack of benchmarks which I have referred to already, lack of training perhaps. We have had a look at Government officials before us; some of them have been very strong in their views as to what they can do and think that they can use their powers for any crime in sight which is worrying. The lack of training, the difficulty of the decisions—they are not easy decisions—has any thought been given as to how you ensure that those who exercise these powers have the necessary training to take not easy decisions?
Mr McNulty: I think we are relatively comfortable with the level of senior management on which these serious decisions are made, but like a lot of activities out there in the broader domain it is when the ability to utilise that power trickles down to the front line, as it were, that I think there may be broader concerns. That is certainly something I am keen to meet both with Sir Simon and with the Local Authority Coordinator of Regulatory Services (LACORS) to discuss this with them. I fear that if there are people pushing at the edges it is with or without the licence of those senior managers who do the signing off and we need to bottom that out and make clear which it is. I do repeat that these are very, very sensitive and serious powers that if, at the edges—as you describe it—they are open to misuse go to challenging the entire integrity of quite proper use of these powers by local government and other regulatory authorities.

Q944 ***Lord Rowlands:*** Is it not the culture of the agency or department? You can have a department which quite rightly focuses on delivering a better set of services to the citizen and therefore automatically coming to the conclusion that the more information they can gather, the more data sharing you can take, that that will be a great facilitator of great services and there is no-one in that department or agency who will ask about privacy, the other side of the coin.
Mr McNulty: I am not sure that that is the case. Certainly from the Home Office's perspective and the prime minister's perspective, notwithstanding the sensitivities around these matters, they are convinced that data minimisation—another ugly phrase but it will do—should be the starting principle, that is: what data does a department or particular aspect of Government require to provide a service, deliver goods or whatever to the citizen? It is not: let us take all the data and then we can work out what we need to utilise to deal with and discharge our functions as a department.

Q945 ***Lord Rowlands:*** Do you think there is a belief in privacy and a culture embedded in government departments?
Mr McNulty: I think there is an increasing culture of being alive to the impact of surveillance and data collection and a guiding principle of greater data minimisation. So the starting premise is to resist the function creep and the data creep.

Q946 ***Lord Peston:*** Can I ask you to reflect on the following? Most of us are older than you but if I had been told when I was a young man that there would come a day when my local authority would actually want to know the details of what I put in my rubbish bin—or in my case in my three different coloured rubbish bins—I would have said you were mad, that we would never come to a state of affairs where that would happen. Why would they remotely feel that that was fundamental to their delivering a service that I want? We now live in a society where there is not only that but they engage in really detailed scrutiny of what we do with our rubbish. There may be arguments in favour of that but in terms of respecting one's privacy I would have thought that that is a cause for concern, particularly given the threatening nature of some local authorities. I keep asking my wife if a bit of plastic goes in the black bin or the blue bin because I cannot remember the difference between the different types of plastic. According to my local authority I would be breaking the law if I put it in the wrong dustbin. Is there not a serious issue of privacy here where one wonders whether anybody in local authorities has thought about that, following Lord Rowlands' point?
Mr McNulty: I think there is and I think there will continue to be—which is why I welcome the debate rather than traduce it—a clash of particular policy outcomes. Twenty or thirty years ago people said you were mad if you thought that unless we do something

rather starkly about the environment the planet is going to perish.

Q947 ***Lord Peston:*** We do not want to argue about that now.
Mr McNulty: It all goes to the same point; that is precisely what I am saying. However small a contribution, you putting the right rubbish in the right bins so that it can all be duly recycled is all part of that process. That is not to excuse a threatening paraphernalia around that if the public officials are discharging their function, but I think the privacy—to back to John Stuart Mill and your private circles—around how you discharge your rubbish has gone back to a public realm in terms of the utilisation of recycling that rubbish. It is a very, very interesting debate, but it still does not excuse the threatening or intimidatory nature of discharging those duties by local councils. I would accept that point.

Q948 ***Viscount Bledisloe:*** You said that the local government official ought to consider whether he needs this information to do his job, but is there not another question there? If I am the dog fouling officer I would need information about dog fouling to do my job, but somebody might say, "Well, maybe, but dog fouling is not that serious that we ought to be spying on people to get it" and you cannot expect the dog fouling officer to make that decision, can you?
Mr McNulty: No, and he would not. Under our architecture a senior manager way above him would, not the operative on the ground floor. I was going to say that I would not poo-poo the notion—I apologise for the pun—but if the one local park available to the community is festooned with irresponsible dog owners who are just using it as an open lavatory for their dogs then the impact of that on children and others in the area can matter. I am not saying it matters in every single circumstance however.

Q949 ***Viscount Bledisloe:*** There are some offences that are not worth the invasion of privacy involved in spying on them. Dog fouling may not be one of them.
Mr McNulty: It is a balance and it does go to the broader point about proportionality, but in the example I think there may be a reasonable and rational application of the law. We are at the edge, I do accept that. Are there circumstances in which I think it absolutely appropriate to utilise the powers afforded to local government against littering? Probably intuitively not, but there might be a broader context where it is absolutely a plague in a particular area so it does go to context and proportionality and the priorities of the local councils and the impact of the misbehaviour on the local community. I would not necessarily trivialise any application, but I do absolutely think—which is why I will discuss it with the commissioner and Sir Simon—that we need to re-define the edges.

Q950 ***Baroness O'Cathain:*** In what ways, if any, do you think that the work of the surveillance commissioners could be improved? Is there a case for requiring them to investigate specific cases where it appears that RIPA powers are being used unnecessarily or disproportionately?
Mr McNulty: It may be and I think the fairest point is to say that the whole commissioner architecture is relatively new and in this area we should keep it as flexible and dynamic as possible to see where the interventions of powers should be. It is certainly a question I will ask the Surveillance Commissioner when I see him specifically about RIPA but I think it is something that the Prime Minister is very keen on too. He will ask the relevant commissioner to look in more detail at the National CCTV Strategy and how that Strategy fits in with where we are at. I would say at this stage, so long as we keep an open mind and be flexible and not lock in a box the definition of what the commissioners should or should not do and constantly go to battle with them if they want to do any more, I think that would be an irrelevant and not terribly helpful approach.

Q951 ***Baroness O'Cathain:*** That would also be covered, of course, if you propose post-legislative scrutiny and watch developments all the time because there might well be technologies which we could not even dream of.
Mr McNulty: I think the Prime Minister in his speech last week formerly asked I am not sure whether it was the Surveillance Commissioner or the Information Commissioner to do an annual report to Parliament to assist that broader post-legislative scrutiny type approach. He did not promise this because he is in awe of the business managers, as am I, but hopefully with a detailed debate on it as well rather than just another document lodged in the library.
Chairman: Lord Smith?
Lord Smith of Clifton: I think most of my questions have been pre-empted by earlier debates so we should move on.

Q952 ***Lord Woolf:*** Moving to a different area, the National Identity Scheme Delivery Plan suggests that there will be the strongest possible oversight of the Scheme. Can you clarify what will amount to the strongest possible oversight?
Mr McNulty: I think the commissioner will have specific and broad responsibilities for overseeing the work of the Scheme. The information commissioner will ensure that there are high standards of data adhered to. We mean it when we say that there should be the strongest oversight possible. Also I think with increasingly a duty to focus on and resist data

maximisation and the notion very alive when I took the Bill through of function creep. The oversight will be as broad as possible. We appreciate it is a serious step.

Q953 ***Lord Woolf:*** Will the commissioner have sufficient resources to carry out this function?
Mr McNulty: Yes, I believe so, and I think crucially including the right to be consulted about changes, not least changes in terms of function and data which of course needs to be approved by both Houses in the first place but I think it appropriate that the commissioner is consulted on that potential change before each House is troubled by orders.

Q954 ***Lord Woolf:*** Of course there will be also the Information Commissioner; how are they going to define the boundaries of the responsibilities of each?
Mr McNulty: I think overwhelmingly the Information Commissioner's role is in the context of the individual data protection and that is very, very clear, whereas the Scheme Commissioner's role will be about the proper oversight and integrity of the Scheme itself and making sure it complies with legislation and that any changes afforded are dealt with and discussed. He will have a role specific to the Scheme whereas you will appreciate the Information Commissioner's role is a far broader remit.

Q955 ***Lord Woolf:*** Who is going to tell them those are their respective roles?
Mr McNulty: Hopefully they will already know. The Information Commissioner certainly knows his role already and I think in the legislation the Scheme Commissioner's role is pretty well defined. It may well be one of those 74 areas yet to be fully defined in one of the orders hanging off the Christmas tree. It is some time since I did the ID Cards Bill so if that is wrong I will get back to your Lordships.

Q956 ***Lord Woolf:*** It may well be that it is best left to them to work it out in practice.
Mr McNulty: That may well be so. I know that because their areas overlap so readily the Intelligence Service and the surveillance commissioners do meet fairly regularly to determine their boundaries. Quite how they relate more readily to the overarching role around the individual data protection of the Information Commissioner I think is a moot point.

Q957 ***Chairman:*** Can I turn to closed circuit television? One of the recommendations of the National CCTV Strategy of October 2007 was for a national body responsible for the governance and the use of CCTV. Could you tell us a little more about this initiative and whether you think there is scope for statutory regulation in addition to better governance, codes of practice and the Data Protection Act?
Mr McNulty: There may be in terms of the second one. In terms of the first point, at the moment there is a programme board looking at the establishment of that national oversight. It contains a whole range of representatives from the Association of Chief Police Officers, the Home Office, our non-departmental public body, the National Policing Improvement Agency, the Local Government Association, the Ministry of Justice, the Information Commissioner's Office and a range of others across Government looking to get in place that national oversight and the broad development of CCTV. I think it is appropriate and that is why we endorse the Strategy because like a lot of these issues CCTV covers a relative multitude of sins. As I referred to earlier when looking at the original concept of a surveillance society you would be forgiven for thinking, given some of the coverage, that every single camera was organised and there and manifestly there only for the state which is not the case; some 80 per cent plus on estimate are private. We think there is a reasonable relationship—whether people know of it sufficiently or otherwise is again a moot point—between the data protection legislation and an individual's rights vis-à-vis cameras, but that might be worth exploring in some more depth. There is also a range of technological capability around many of the cameras, most of those in the public space domain may well retain images for up to a month; many, but not all, of the private ones are at their most basic on a sort of 24 hour loop and are constantly taping over the images recorded. I think it may well be that this national body as it goes forward does look at the relationship between individuals, public authorities and CCTV. This area, above most, and the DNA database are areas where I would traduce entirely the big brother image because it is a nonsense.

Q958 ***Chairman:*** What would you think, Minister, of the suggestion that the Information Commissioner or another similar person should have to approve major new CCTV schemes or carry out retrospective inspections in the way the surveillance commissioners examine the use of RIPA powers?
Mr McNulty: I am not sure how helpful that would be unless we discern a difference between different types of CCTV schemes. It may well be that new schemes put in a town centre now, for example, will be wholly different from one that has been there for ten or 15 years and can have considerably more technological capabilities that may go to both better protection and have potentially greater intrusion so that there might be a case for doing that looking forward, but I am not entirely sure what a retrospective view of even those public place and space camera systems or indeed private would achieve because invariably things have moved on so readily in terms of the technology, so your

benchmark for assessing the impact of something retrospectively would be almost irrelevant.

Q959 ***Lord Peston:*** Going back to Lord Woolf's question, it suddenly dawned on me that I am totally ignorant now of where we are on the practical introduction of identity cards. You mentioning the 74 branches of the Christmas tree worried me. Would it be possible for your Department to give us a short statement on the present state of play, where we are with identity cards?
Mr McNulty: Of course; that is entirely reasonable.

Q960 ***Baroness Quin:*** You mentioned earlier the principle of data minimisation. I think the Home Affairs Select Committee is also keen on that principle. How does that apply to the National DNA Database, in particular in keeping DNA information on persons who are not charged with or convicted of an offence? What about the time honoured principle of presumption of innocence here? Is it fair to treat people who have never been charged or convicted in the same way as those who have been?
Mr McNulty: I think there is an entire misunderstanding of the nature of the National DNA Database; there are no guilty people on it in the sense of guilty of future charges. It is not an information source for all the naughty and potentially nasty people in the country and if you are on it is a stigma. It is purely an informational and investigatory device for the police. I would, I think, defend absolutely the position we are in now. You will know there are those who say why not go straight to a universal database. I got in trouble because I rather clumsily said on the *Today* programme that I had some sympathy with the spirit of the logic behind that which, of course, days after was cast as "Government minister has sympathy for universal database" which I did not say; there is some logic to it. I think that would be intrusive and unnecessary and cause all sorts of difficulties. We have also looked at broadening out the potential sweep of the DNA database to all offences recordable and non-recordable, ie every fine and everything else and I think that is a step too far. I think where we are now is appropriate. I do not think it is intrusive and I think collectively in terms of weighing the public good against the intrusion on the individual, the litany of rapists, killers, child abusers who nominally, on anybody's definition, would fall into your innocent category, ie they have encountered the criminal justice system but the case has not been pursued against them, only for it in some cases, 15 or 20 years later, horrendous crimes are to be laid at that individual's door purely because of the individual DNA sample being on the database. If we go back to the notion of balance between the individual and the state, I think that is a balance worth defending and equally in many instances, of the 40,000 or so crimes dealt with since the inception of the DNA database, in any number of cases the police would have been able to entirely eradicate someone whose DNA sample was at a particular scene for entirely innocent purposes but they would only have been able to do so because they had that sample on the database as well. I would passionately defend the position we are in now in terms of the DNA database. The list of rapists, killers and everything else we have resolved only because of the existence of those samples on the database puts for me the balance very, very firmly into the maintenance of the database as it is now.

Q961 ***Baroness Quin:*** Given that you have talked about cases that have been solved 15 or 20 years later, do you have a view as to the time period after which DNA information should be deleted?
Mr McNulty: At the moment it is not, as you will be aware. Tony Lake, the outgoing Chief Constable of Lincolnshire, who was the ACPO lead on forensics, is looking at whether there should be, particularly for younger people, a time limited period of retention and then subsequent deletion. We are trying to explore that with him at the tail end of the broader PACE review. I think that sort of element is worth exploring, especially for very, very young people, but I do want to get away from this notion that somehow these are individuals who, if we have not get them yet we will do, so they are almost a nearly guilty. It is not a list of either guilty or innocent or anything else; it is simply those who, for whatever reason, either at crime scenes or in terms of arrest but not ultimate conviction, have encountered the criminal justice system and it is a very, very useful investigatory and information device for the police and should not be seen as anything other than in those terms.

Q962 ***Viscount Bledisloe:*** I understand the point that everybody should be on the National DNA Database. I can understand another position which says that anybody who has been convicted of a criminal offence—or offence of sufficient importance—should be on. How can it be right to keep the DNA of somebody who has been taken but was not in fact guilty of that offence and the DNA was taken for the purposes of eliminating them from the enquiry? How can it be right that against their wishes—or certainly without consulting their wishes—it is retained?
Mr McNulty: How can it be right? Because it is not a sign of guilt; it is purely informational. I agree also with the logic of a universal database and can see the integrity of such a logic, but I do think for all sorts of reasons that is a step far too far, as is the broadening out to non-recordable as well as recordable offences. You have to strike a balance in these things and I think the balance is about right.

Q963 ***Viscount Bledisloe:*** If two people are present at a place where a murder has taken place and one of them voluntarily gives his DNA because he thinks it will help the police and the other one refuses, you keep the man who was cooperative but the man who refused is not on your database.
Mr McNulty: Unless he is arrested subsequently for anything else.

Q964 ***Viscount Bledisloe:*** Yes.
Mr McNulty: It is not about eliminating everyone and finally having everybody on the database. It is, by its nature, to an extent arbitrary in the terms of it being restricted to those who encounter by arrest or for some other reason a crime scene, but is a strong place to be in. I do not think there is a matter of principle here; I do not think there is any stigma attached at all with being on the database. The whole notion of "Can we take the innocent off the database?" is, when you think about it, abject nonsense because there is no guilty on the database. There may be people who have been guilty of other crimes in the past but on one level the intrusion into their liberty, just because they have committed an offence they should be on the database, is just as potentially damaging as the "complete innocent". The power of the DNA database I cannot overestimate in terms of some of these cases. To give an example, Stefan Kisko only came out of prison because of a DNA database sample that Ronald Castree had had but it was years before he was arrested and convicted for that particular horrendous crime. I am not saying all 40,000 crimes that have been successfully dealt with because of the DNA database are as horrendous and as headline in nature as the starker cases but I think it matters. Dealing with these very, very serious crimes and getting innocent people incarcerated off because of it in some cases does matter and it is a matter of public policy and that balance between the individual right and public policy; this is actually something where the public good does outweigh the inconvenience of people being on the database if they have ever encountered the criminal justice system. I do believe that profoundly but there are people running around the country on some sort of campaigning charging white horse trying to get people to knock down the National Database or somehow take the innocent out of it. There are some horrendous cases here of the innocent who, by some of these people's definitions, would be now out of the frame absolutely in terms of being charged with their horrendous crimes.

Q965 ***Viscount Bledisloe:*** Do you realise that inherent in that whole observation was the theory that you do not get investigated by the police unless there is something wrong with you?
Mr McNulty: Absolutely not. You are not investigating everybody on the database because they are on the database. You are investigating DNA samples found at crime scenes in the absolutely normal fashion of investigation and if, by chance, for some other entirely erroneous reason that perpetrator happens to be on the database they will be charged accordingly. It is not fishing. It is not a case that we have all these people on the database, they all must be guilty, now let us find a crime to attach to them. In terms of the wider political domain that is exactly the sort of sloppy intellectualism that attracts itself to this that I profoundly disagree with because of the profound power of dealing with these individual cases. They just will not happen, full stop. They will not happen unless we do have a database that has to be populated in some arbitrary fashion, yes it is populated by samples from crime scenes and you will remember in the past the home secretary did take samples from the entire prison population at that particular time and topped up by anyone who encounters the criminal justice by arrest. That is not to say they are guilty or otherwise; it is purely a very powerful informational diagnostic tool that I would utterly defend.

Q966 ***Lord Woolf:*** I gave a judgment—I have to disclose this—absolutely upholding the position you have just described and the case that was put against my judgment is that we really are adopting a totally illogical position. If your arguments are as powerful as you suggest they are, then surely they are powerful arguments in favour of universal disclosure. If it be the case that they are powerful arguments about universal disclosure where we all do it, then there is no inference that you are almost guilty or anything of that sort. What are the arguments that have persuaded you against universal? Why is too far?
Mr McNulty: As I say, I fell into the trap courtesy of Mr Humphries or whoever by saying that I agreed with the very strong logic of a universal database but I think it is outweighed by practical civil liberties and potentially legal concerns—notwithstanding the European court case that is before the courts at the moment—that prevail against that.

Q967 ***Lord Peston:*** And costs.
Mr McNulty: Yes, absolutely. The costs and practicalities as well, but in the sort of broader public policy and philosophical context of course I see the logic of it but I do think there are cost practicalities, legal and civil liberties dimensions that prevail against it, although I do see the logic. That was the trap that Mr Humphries drew me into.

Q968 ***Lord Woolf:*** I do not think it is right to say that it was a trap; it is a question of facing up if it were so beneficial for the public interest. Can you give some

indication of what would be the additional cost of everyone being required to disclose their DNA? It is a very simple exercise.

Mr McNulty: I do not think to either cause excitement from media colleagues behind me or a nervousness in other people, that there is some report or work that has been done by Government to look at the costings for taking and then storing individual DNA for everyone. I think there are strong civil liberties and other reasons why, notwithstanding the logic, it is not a road I would go down. Some police officers do put that forward, and some a much wider base than we have now. You have to draw the lines of parameters somewhere and I think the line that says that encounter or arrest in the first instance is a sufficient line to draw for recordable offences, not just every offence. On a logical level I to take the broader point, but I think there are powerful public policies and civil liberties that in the balance of things mean that the position we have now is preferable to that sort of universal approach.

Q969 ***Lord Rowlands:*** We are still trying to grapple with the simple proposition that I, as an individual, volunteer to give my DNA—I am not approached by the police, I volunteer to give my DNA—why do I not have the right to say that afterwards I wish to have it eliminated?

Mr McNulty: By the nature of it and by the nature of the logic we have just been discussing, the DNA database is more enhanced with your sample on it than not. As I say, the work we are doing with ACPO to look at potential retention periods, especially for the concern—I put it no stronger than that—about very, very young people being on it and we do need to get to an acceptable and agreed position on that.

Q970 ***Lord Rowlands:*** Will you get a better voluntary effort if you at least give the citizen the right afterwards to say that he now wishes his DNA to be eliminated?

Mr McNulty: It is interesting that what there has not been is any concerted effort by Government to get voluntary contributions to it; maybe that is an area we should explore and then look at the retention protocol around that. The notion that volunteers should have at least the option for retention being for a shorter period than forever is a fair one that we are exploring.

Q971 ***Baroness O'Cathain:*** Still on the same question really but I take a somewhat different view. I do not know whether the Government has looked at this, there does not seem to have been much publicity about it, but a lot of women particularly would feel a lot more secure and safe if everybody was on the DNA database, particularly in rape cases, because there is a universal feeling out there that women who are subjected to rape do not have any chance whatsoever of getting any sort of justice.

Mr McNulty: I think the corollary of that is how some significant major rape cases have been dealt with only because of the DNA database so it goes to the same point. The debate around universalism will continue. In many investigations up and down the country around rape a goodly number—if not the overwhelming majority of the male population in a particular area—have come forward quite willingly to submit their DNA sample to be eradicated. I do not think it is a debate that will go away. I think the position now is a very, very powerful one and I really would traduce those who are in opposition to it. I think there are principles around where you draw the line, but I do not understand at all these white knights charging round the country on some sort of civil liberties campaign saying that the DNA database is somehow inherently evil. That is an absolute nonsense. I have had some assistance from behind me—you get these inspirations every now and then—says: "Volunteer samples may only be taken where the person provides written consent to give a DNA sample to assist the police investigation. The resulting DNA profile is then compared in a forensic laboratory with the DNA material recovered from the crime scene. Volunteer profiles are only added to the National Database where an individual has given separate written consent for the profile to be loaded and retained. The consent form explains that once consent for addition to the National Database is given it cannot be withdrawn." That reinforces your point and it is something that we do need to look at in terms of Tony Lake, the ex-head of Lincolnshire who was the ACPO lead on forensics and his successor. Regulating the framework roughly where it is now I think is hugely important and I have a task to explain to more and more people the public policy benefits of the DNA database and some of these significant cases only coming to fruition and conviction of the perpetrators because of an "innocent" sample given some time before the individual is actually caught on the major crime. That is a huge debate.

Chairman: Minister, thank you very much indeed for joining us this morning and for the evidence you have given.

Supplementary letter from Tony McNulty

Following my appearance, I said that I would write to the Committee in response to matters raised by the noble Lord, Lord Rowlands on the written evidence submitted by Dr Pounder.

Lord Rowlands raised the issue of Dr Pounder's contention that widely drawn primary legislation can result in the use of secondary legislation to modify the intention of the original provisions of the Act; and Dr Pounder's questioning of the ability of Parliament to scrutinise any legislation effectively.

These are significant charges and as I indicated in my response to the Committee, Dr Pounder's view is fundamentally wrong. His reference in his evidence to the Committee to the Identity Cards Act 2006 is a prime example where we have a number of order making powers, in fact some 74. However, what he fails to acknowledge is that these must comply with sections one to three of the Act which clearly define the statutory purpose of the National Identity Register and the information that it may hold.

If we wanted to amend the statutory purpose of the National Identity Register, then we would have to amend the primary legislation and not, as his evidence suggests, introduce change by way of secondary legislation.

Dr Pounder also makes reference to the Children Act 2004 and the Anti-Terrorism, Crime and Security Act 2001. In the case of the former, the 2004 Act is again explicit on the face of the Bill in setting out the contents of regulations. For example, section 12 provides for regulations on Information Databases and is explicit on both the categories of information that can be gathered and the extent of regulations on how can access the information.

The order-making provisions of the Anti-Terrorism, Crime and Security Act 2001 relating to the security of pathogens and toxins similarly set out parameters on the face of the Act. The order-making power which allows the Secretary of State to I modify Schedule 5 to the Act is restricted in that a pathogen or toxin may only be added to that Schedule if the Secretary of State is satisfied that it could be used in an act of terrorism to endanger life or cause serious harm to human health. This order-making power is subject to the affirmative resolution procedure.

Clearly there are significant statutory safeguards in place which hold the order making process in check both in compliance with requirements set out in primary legislation and, importantly, by virtue of approval of each House of Parliament. We will continue to adopt that approach.

I also agreed to provide a briefing on the current state of play with the National Identity Scheme, which I attach (Annex 1).

22 July 2008

Annex 1

THE NATIONAL IDENTITY SCHEME

— The Government was elected in 2005 on a manifesto commitment to introduce identity cards and Parliament approved the Identity Cards Act 2006 in March 2006.

— Research (February 2008) shows that 59% of people support the government's National Identity Scheme. The British Social Attitudes Report published in January 2007 showed that 71% of people think that having compulsory identity cards for all adults is "a price worth paying" to help tackle the threat of terrorism.

— 24 of the 27 EU member states already have ID cards -all apart from the UK, Ireland and Denmark—and Denmark has a national civil register which requires all residents to be registered and to be issued with a unique identity number.

— Biometric identity cards will provide a secure way for people to prove their identity securely and reliably as well as helping to combat immigration abuse, illegal working, identity fraud and crime, strengthening national security and improving access to public services—will support transformational government agenda.

— Facial image and fingerprint biometrics will link an individual securely to a single unique identity and prevent people enrolling multiple identities. All British passports (six million per year) are now e-passports with a facial biometric included in a chip in the passport booklet.

— Everyone issued with an identity card will have their identity details, including photograph and fingerprint biometrics, held on a National Identity Register and will be issued with a unique National Identity Registration Number. Notification of changes to name or address will be required so that the Register is kept up to date.

— The National Identity Scheme Delivery Plan was published in March 2008 (http://www.ips.gov.uklidentity/downloads/national-identity-scheme-delivery2008.pdf) set out the government's plans to provide more secure and reliable ways of proving identity, including more secure biometric passports and the introduction of identity cards.

— The plans are for the UK Borders Agency to start to issue biometric immigration documents, known as identity cards for foreign nationals to non-EEA nationals from 2008 using powers for compulsory cards for foreign nationals contained in the UK Borders Act 2007.

— The Identity and Passport Service will begin to issue the first identity cards to British citizens from 2009.

— In the latest National Identity Scheme Cost Report [8 May 2008], the Government confirmed that it has made savings of almost £1 billion in introducing the NIS against the last cost estimates.

— The total estimated cost of the scheme for the next 10 years is £4,740 million for UK citizens, including the issue of both passports and identity cards, and £311 million for foreign nationals.

— The foreign national costs have risen from £182 million to £311 million as we will be issuing more cards to more foreign nationals. These costs will be fully recovered from fees charged to foreign nationals.

— Approximately 80% of this cost will need to be spent in any event just to implement secure biometric passports and as with passports, the operational costs of issuing ID cards will be recovered from fees.

— It is intended that the fee for a British citizen's identity card issued in 2009 or 2010 will be £30 or less.

— Further information may be found the National Identity Scheme Cost Report:

— http://www.ips.gov.uk/identity/downloads/IPS-Identity-Cards-Scheme-CostReport-May2008.pdf

— A National Identity Scheme Commissioner will be appointed to oversee operation of the Scheme and report annually on the uses to which identity cards are put, the confidentiality and integrity of information recorded in the Register.

— Information may be provided from the Register with individual consent to confirm identity to private sector organisations or without consent to police, security services and government departments or public authorities approved by Parliament.

— The Identity Cards Act excludes any requirement to have to carry an identity card at all times and made no changes to police powers.

— It would require further primary legislation in the future if it were eventually to become compulsory for everyone aged 16 and over who is legally resident or working in the UK to have an identity card, and for it then to become a requirement to produce an identity card when seeking employment or accessing public services.

— Updated National Identity Scheme Strategic Action Plan published on 6th March set out the roll out as follows:

  — 2008—Begin to issue compulsory identity cards to foreign nationals (start with foreign students);

  — 2009—Issue identity cards as part of improved pre-employment checks for people employed in positions of trust—such as workers at an airport who need identity verified to a high standard;

  — 2010—Start to issue identity cards on voluntary basis to young people (16 to 19 age group) to assist them in proving identity; and

  — 2011/2012—roll out large numbers of identity cards linked to the introduction of fingerprint biometric passports.

— We will start with rolling out cards where there is maximum benefit in terms of protecting the public—hence starting with foreign nationals and then people employed in positions of trust.

— Once fingerprint biometric passports are introduced to give everyone the choice of having a passport or identity card or both, with identity details and biometric recorded on National Identity Register.

— Working closely with the private sector to help reduce the cost of the scheme (such as for enrolment of fingerprints).

— Working to build public trust by explaining how the scheme will work—only minimal amount of identity information will be on Register, much as currently held for passports and immigration documents—together with an audit record of whenever a person's record is accessed.

— We will make the most of the oversight from new National Identity Scheme Commissioner as well as existing Information Commissioner and will consider a panel of users and the public.

Examination of Witnesses

Witnesses: MR MICHAEL WILLS, a Member of the House of Commons, Minister of State and MS BELINDA CROWE, Head of Information Rights Division, Ministry of Justice on the Surveillance Inquiry, examined.

Q972 ***Chairman:*** Good morning. Can I welcome very warmly to the Committee the Minister, Michael Wills, and Ms Crowe. We are being televised so could I ask you please to identify yourselves for the record and then the Minister will make a very short opening statement.

Mr Wills: Thank you very much, my Lords. I am Michael Wills; I am the Minister of State in the Ministry of Justice with responsibility for data handling issues. On my left is Belinda Crowe who is the Head of Information Rights Division within the Ministry and who has responsibility for a team of officials who deal with these issues not only within the Ministry of Justice but provide advice and support throughout Whitehall as well. Thank you for this invitation to come here. It is a timely meeting because today we are going to see the actual results of one of the reviews that was set up by the Prime Minister towards the end of last year looking at a whole range of data handling issues, reviews into what has happened in the Ministry of Defence, in HMRC and across Whitehall as a whole. What these reviews reflect in a fundamental sense is what a huge challenge data handling has become for all organisations. This is not just the public sector, it is the private sector as well. Technology has moved so dramatically fast that organisations are really struggling to keep up with the implications. The advantages of what these new technologies offer are manifest and developing all the time, but the consequences of how data is handled are really also dramatic and organisations have found it difficult to keep pace. As I say, there have been some very well publicised incidents within the public sector, but the private sector is not immune from this as well and there have also been some slightly less well publicised incidents. A lot of financial institutions have had catastrophes with data handling. Mobile phone companies, retail companies, all of whom keep and use huge quantities of data, when you talk to them they will all say how valuable this is to them but there are consequences for how they protect the privacy of their customers' information and for the public sector the burden is equally intense. We are running to keep up and that is the lesson that I have certainly come away with from my last year in this job. The advantages of these new technologies and what they offer in terms of data sharing are immense, and I may come on to that in response to some of your questions. It is clear that we do need a radical change of culture within Government about how we handle data. Over the years I think Government has become very scrupulous about how it handles money; there are very clear systems of financial accountability and transparency in place and everybody realises the need for that. I think the case with data is less clear. Clearly we do not handle data in the same way as we handle money and we should. That is the cultural challenge that all of us face—ministers, politicians and officials alike—and that is the challenge with which we are now grappling.

Q973 ***Chairman:*** Can I just press you a little further on that? Apart from the issues you have touched on, certainly the security of personal data against loss and breaches, how satisfied are you that the development of Transformational Government has resulted in the Government that you have touched on that minimises the collection of these data and processes them in line with the spirit and not just the letter of the Data Protection and Human Rights Acts?

Mr Wills: I think by its very nature the Transformational Government agenda should implement the minimisation of data principle because what it is trying to do is to use data more efficiently so instead of having a lot of separate and often quite large databases we are trying to integrate them. That should actually minimise these separate databases and ought to improve the security and handling of data, but it is not a panacea on its own. Its primary motivation is to improve delivery of public services for the citizen and all the other things that are necessary for the security and proper handling of data have to be put in place. It is not a solution to it but I think it is absolutely consistent with the minimisation of data principle.

Q974 ***Chairman:*** Apart from the Government's Information Sharing Vision Statement what did the Ministerial Committee MISC 31 achieve in attempting to resolve cross-governmental disagreements and fragmentation concerning data sharing and privacy? Why was it dissolved before announcing any final solid policy conclusions? What lessons, if any, have been learned from this episode and what plans are there for the future?

Mr Wills: It pre-dates my time in this role so, if I may, when I have made a few responses to your various questions I will perhaps ask Belinda Crowe to add from her own experience of MISC 31. It was, as I understand it, an attempt to bring together across Government all the ministers with responsibilities in this area to see how we could join up what we do in this and that is clearly crucial. I think everybody accepts that collaboration across Government in these issues is vital. There have been some very good examples of it and I think MISC 31, from what I have seen, did do a good job in starting a process of collaboration across Government. It became

overtaken by events and perceptions that we needed to look at this afresh when this prime minister took office before the very well publicised incidents of data loss and, as it were, inadvertent data sharing. He felt there were real issues that needed to be addressed here and that is why we set up some of these reviews before these incidents took place, such as the Walport/Thomas review. In answer to your question I think it did a valuable job in promoting collaboration. Some of the fruits of it we are still taking through and I will perhaps allude to those in response to later questions. However, that mechanism needs to be updated and what we are planning to do is to wait for the results of the data handling review that is being published later today, the other reviews will follow shortly afterwards. Once we have got those reviews and have taken stock and evaluated them then I think we will have to look at a new mechanism that promotes that sort of collaboration.

Ms Crowe: I would just reinforce the point that the creation of MISC 31 and, if you like, the official support that accompanied ministers did highlight the need for greater collaboration across Whitehall in the development of new policies and the way that data sharing and data protection issues were handled across the piece. Certainly in terms of the work that I do, when we looked at what the barriers to data sharing were in order to transform the way that public services are delivered, in actual fact data sharing and data protection was a small part of that and actually the main part was joining up together and different departments working together in order to deliver a particular policy outcome. It started to create a culture shift in terms of collaborative working on these issues which, as Michael says, was then taken forward and actually passed onto the Walport/Thomas review hopefully to feed into their thinking.

Q975 ***Baroness Quin:*** Do you think there is a case for some kind of formal ministerial committee on privacy? In your time in your present post have you had many discussions on privacy issues with colleagues in other departments?

Mr Wills: The answer to the last part is yes because it comes up all the time. When you talk about privacy, there clearly is a role for some kind of formal mechanism for ministerial collaboration on these issues, precisely what it is I think we will have to wait and see what these reviews recommended. That is why they were set up and we will act on it, there is no question about that. It is important that this is not only about privacy, it is also about how we maximise the benefits of data sharing. These are real and I do not think we can ever look at these things in isolation. All of us often want two separate things at the same time. We are all very careful about our own privacy; we want our own personal details to be kept confidential. However, we also want more efficient public services. To give two brief examples, if I may, why this is so important, we know for example that there is a big problem with the take up of free school meals and a lot of young children are not getting adequate nutrition even today in this country because their parents are poor and they are not, for a whole variety of reasons, able to have the free school meals to which they are entitled and their nutrition is, without doubt, suffering as a result. The information that would enable us to identify those young children is available to us and it has taken Belinda and her team quite a long time to find a mechanism by which we can actually share that data so young children can have adequate nutrition. That is a good that everybody can subscribe to but it does depend on data sharing to improve that level of take up. Similarly Sir David Varney when he was looking at this quotes an example of a bereaved family who had lost a family member in a road accident. In these tragic circumstances the last thing you want to do is to be badgered with lots of information. I think they had 44 different contacts with the state in different ways and that is unacceptable. These things need to be done but if you could share the data the level of intrusion into a family in grief is minimised. That again must be a good that all of us could subscribe to but you do need to have data sharing. The question is how do you do that without, at the same time, compromising people's quite proper sense of their own privacy and confidentiality? That is the challenge. When we talk about privacy I think we have always got to balance it with data sharing. We always have to keep the two things in our minds at the same time.

Q976 ***Viscount Bledisloe:*** If I have some information which is private to me surely I am entitled to have that retained absolutely even if you in Government think it would be useful to share with other people?

Mr Wills: Of course there are all sorts of rights to privacy; it is embedded in the Human Rights Act, not the right to privacy as such but certainly something that comes quite close to it. There is a nice legal point about whether there is an emerging right to privacy or not as you will be aware, but certainly of course that is right. However, where the data exists already, where it has been voluntarily given or where, as a society, we have decided it should be given—details about our income, for example, to the tax authorities or whatever—then we as Government have a duty to the public to look at ways in which, consistent with the legislative framework, consistent with the political consensus at the time, we use that data for the benefit of everybody. These are difficult questions of judgment; there are no absolutes here and it has to be done on a case by case basis. I do not think that

these things are incompatible at all. We strike these balances every day in our personal lives as much as anything else.

Q977 ***Viscount Bledisloe:*** You say in your ministerial statement—or it may have been issued before your time—that once information has been collected the Government is very careful to ensure that sharing can only take place when it is not incompatible with the original purposes of a collection. Can you give me any example where sharing would be incompatible with the original purposes of collection? Is it not virtually a meaningless protection?
Mr Wills: I do not think it is a meaningless protection at all; that is embedded in the Data Protection Act.

Q978 ***Viscount Bledisloe:*** Give me an example of where any sharing that Government might do would in fact be incompatible with the purposes for which it was collected.
Mr Wills: Rather than give you a theoretical example, these are the kinds of issues that Belinda Crowe and her team are actually tackling all the time. When she gives advice and support to colleagues throughout Whitehall these are real issues and the advice and support that Belinda and her team give is precisely delineating what is compatible and what is incompatible. I do not know whether this is compatible with the principles we are talking about, but if it were to be compatible perhaps you could give some indication of an actual case that you have dealt with in the last couple of years on this.
Ms Crowe: I might have to disappoint you only insofar as we just would not allow that situation to arise. I think that is the general thrust behind the statement; the statement was meant to be both reassuring but also how in practical effect the policy is developed. A theoretical example, if that will do, might be that if the HMRC were to pass over details of your income to your GP for example; I cannot think for what purpose that might be but HMRC do not collect information about your income for that purpose so it would be incompatible to pass that information, for example, if there were some mean test medical services, to pass that information on.

Q979 ***Viscount Bledisloe:*** I have to say, Ms Crowe, if that is the best example you can give I am not really very deeply impressed. Would it not be much better if the answer was that you could not share my data outside the purpose for which I gave it unless you had my express permission?
Mr Wills: You cannot; that is one of the principles. There are eight principles of data protection and that is one; it can only be used for the purpose for which it was collected.

Q980 ***Viscount Bledisloe:*** Yes but you say it cannot be shared for incompatible purposes.
Mr Wills: The second data protection principle is that it should be processed for limited purposes and shall not be processed further in any manner incompatible with the original purpose.

Q981 ***Viscount Bledisloe:*** Incompatible with, yes.
Mr Wills: I am sorry, I am perhaps missing your concern here.

Q982 ***Viscount Bledisloe:*** If you wanted to give information about who could afford school meals, now the reason the person gave you information about their income was not to do with school meals but it is not incompatible to pass it on.
Mr Wills: The purpose for which the information about income that was given to the local authority, for example, was to receive a benefit.

Q983 ***Viscount Bledisloe:*** That clearly is compatible.
Mr Wills: Yes, that is why it would be compatible. If it was for any other reason than for a benefit from the state then it would be incompatible but that is why it is compatible. If, for example—I am straying into very theoretical territory which I said I would not do here—we had data on people's income and it was handed over to the school which decided it wanted a very middle class selection of pupils for it, then that would be completely wrong. It would be completely wrong if a local authority had collected data for the purposes of, say, council tax benefit and then it handed it over the local education authority because they had decided that, for reasons that they thought was good, they wanted to concentrate resources on poor children and they should all be concentrated in one particular school, in my view that would be incompatible with the purpose for which that data was collected.

Q984 ***Chairman:*** Could I just ask if you could confirm the use of the statutory override in schedule two of the Data Protection Act in the context of what you are talking about?
Mr Wills: I think I will ask Belinda to do that; it is a rather technical question and I will defer to the expert on this.
Ms Crowe: I might need to understand a bit more as to the context.

Q985 ***Chairman:*** The Minister has been saying that the information can only be used for the purpose for which it was given but there is in schedule two of the Data Protection Act a statutory override enabling the information to be used more widely for other purposes.

Ms Crowe: I think we would need to write with information about setting out specifically how that might be used. I do not have that answer at my finger tips.

Q986 ***Chairman:*** Perhaps we could have a written note on that.
Ms Crowe: Yes, of course.

Q987 ***Lord Peston:*** Am I, as an individual person, supposed to know what data the Government collects about me and has?
Mr Wills: You are not supposed to know but you can know if you want.

Q988 ***Lord Peston:*** In my case I do not have the faintest idea what data you collect on me. I know some of us fill out an income tax form each year but it is not my duty to know.
Mr Wills: No.

Q989 ***Lord Peston:*** But I am entitled to know.
Mr Wills: Of course.

Q990 ***Lord Peston:*** Who would I write to? To you?
Mr Wills: To the organisation you think might hold it.

Q991 ***Lord Peston:*** Yes, but I do not know. Who would I write to to ask what data the Government has in total on me?
Mr Wills: How would you go about finding out all the data that is held about you?

Q992 ***Lord Peston:*** Yes, that is the question I am asking you. It is impossible.
Mr Wills: At the moment it is and it is impossible for perfectly good reasons, for the reasons we have just been talking about because data sharing is not universal. There is not a single database where you can just go to and find everything the state holds for good and proper reasons. There is an argument which I think I hear you making and this is something we will want to look at after Walport/Thomas about giving the public more confidence. This is absolutely essential and if part of giving people more confidence is to bring out into the light the fact that the state does not hold all these murky secrets and all these bits of information that you have probably forgotten about yourself but someone somewhere in Whitehall has got it, then I think that is clearly something we must look at. How we do that exactly is going to be quite difficult mechanically because I do not think anyone wants to see gigantic databases where anyone can go and search. The security implications of that are horrendous. Again one has to be cautious about how one does this. There are probably ways in which we can go a long way towards meeting that kind of requirement; that is one of the key outcomes, we hope, from the Walport/Thomas review when they have reported which is about how we balance data sharing and all its advantages with privacy. That question of public confidence is absolutely central. If the public have no confidence in the way data is being handled they will feel much less sanguine about taking the opportunities of data sharing and society as a whole will be poorer. If they have confidence because the systems are robust and transparent—which is also crucial—then of course we can reap the benefits.

Q993 ***Lord Peston:*** You are aware that what I am really asking you about is privacy, but my problem is that I do not know whether the data on me is accurate. I remember the first time I went as a student to America 50-odd years ago and I was asked what I did. I said, "I'm an economist" and the chap wrote down "He is a communist". I just managed to catch that he was writing it down when I said it was not quite the same thing. The real point I would have thought the ordinary person is worried about is partly data sharing but if you are also sharing dodgy data then they are even more worried about it.
Mr Wills: Yes, and you have a right to correct the data. The crucial point is that you only have the right to correct it if you know it is wrong.

Q994 ***Lord Peston:*** You have to know it is there.
Mr Wills: You have to know it is there and you have to know where to go. We are in an imperfect world in this and that is absolutely right. If we are worried in a specific area then the remedies exist. If you have access to it then the remedies exist to correct it. The problem is that not everybody knows everything that is held and I accept that point. That may turn out to be crucial to public confidence and I expect it will play an important part in generating public confidence. There is a great unease about the spread of people holding data about you but it produces huge benefits in the private as well as the public sector and it is not just the public sector we are talking about here. Your credit references are also very important as well, but people tend to worry about that and that tends to be brought to light quite quickly and that culture is changing. There is a job there and after Mark Walport and Richard Thomas have reported that is clearly an issue we are going to look at.

Q995 ***Lord Rowlands:*** There is a growing movement towards the application of privacy impact assessments (PIA) and the Information Commissioner is keen on them as long as they are not just tick box. Some of us went to the United States and had a meeting with the Chief Privacy Officer and his team in the Department of Homeland Security. There is a mandatory requirement for PIAs in the

United States. First of all, what are your thoughts about the development of PIAs and, secondly, what about the mandatory requirements?
Mr Wills: We are very keen on it and every major gateway project in Government will now have a privacy impact assessment attached to it. We are keen to see them rolled out; we think they will perform a very valuable function.

Q996 ***Lord Rowlands:*** Will these be in the public domain?
Mr Wills: Yes.

Q997 ***Lord Rowlands:*** What about the mandatory requirement? Do you think we should go further?
Mr Wills: I think in essence we have said we have now pledged to do this so every major project will have one.

Q998 ***Baroness Quin:*** Will pieces of legislation have a privacy impact assessment?
Mr Wills: We have not gone as far as that yet and it will depend I think on the piece of legislation. There will be legislation which is just not relevant. My own personal view is that Government should be doing this. Again, we want to take stock of Walport/Thomas which is looking at precisely this area but it is quite clear that where the privacy impact assessment is at a place that we want to be—in other words it highlights the importance of this and it is crucial to keeping public confidence in the way that Government holds data—without wishing to commit precisely to every piece of legislation having it, we are wholly sympathetic to the purpose of it and depending on exactly what the Walport/Thomas review says we will be meeting those objectives in some form or other.

Q999 ***Lord Rowlands:*** On the back of this may I ask a supplementary question and that is that we have received quite a lot of evidence from a considerable number of witnesses who expressed the view that the Information Commissioner is under-funded and indeed also needs further powers. Is the Walport/Thomas report going to review himself and his resources and power?
Mr Wills: We constantly review his resources and he is actually funded directly by the data protection fee. I think when he talks about under-funding he is referring to his freedom of information work. This is quite a complex issue, I have to say. We have found, since I have been in this position, a lot of extra money for him. It has gone up by over ten per cent this year.

Q1000 ***Lord Rowlands:*** He is funded from the fees?
Mr Wills: He is funded directly from the fees and as far as I am aware he feels that is an adequate resource. In my many discussions with the Information Commissioner about his funding—I stress the word "many"—he has never, from memory, complained about the data protection funding which is separate from the FOI funding. He has frequently raised issues about his FOI funding but all things to do with money are slightly complicated and I would just say that we have found an increase of over ten per cent in the last year at a time when all government departments are finding their budgets very stretched indeed, and this Department as well. There are other measures that we have suggested he might want to take to help clear his backlog, to do with different ways of running his office which are under continuing discussion. We have also arranged secondments from Whitehall departments to help with his human resource; indeed, there is a secondee from the Ministry of Justice already there. We recognise his views on this; we are trying to meet them. Freedom of information is enormously important but that is where the issue is, not in terms of data protection money.

Q1001 ***Lord Rowlands:*** Highlighting the dual role he has reminds me that in our Canadian discussions the Canadians were adamant that these roles were basically incompatible, that there could be a conflict of interest between the FOI role and the data protection role. They would not have an information commissioner combining both those roles. Do you think there is any case for splitting those as well?
Mr Wills: There is always an intellectual case for changing the machinery of government and public bodies. I would not say there is no case for it but I have to say I think he has done a very good job and he and his team do really a very good job in what are still relatively new areas of public policy. They have been extremely robust and the way they have operated has not always been comfortable for Government, but they have done an excellent job. Richard Thomas and his team are consummate professionals. Whether as a minister or as a backbencher or as a citizen I have seen no problems and no conflicts of interests at all. Belinda has been at this rather longer than I have, would you agree with that?
Ms Crowe: Yes, I would agree with it and I believe that Richard himself finds the roles sit quite well together. Indeed, in many speeches he has made he starts off by saying that intellectually there might be some inherent tensions but from a practical point of view this is about a regulator looking at the way people exercise their information rights on the one hand openness where appropriate and protection where it is necessary.
Mr Wills: To answer your first question about the powers, we think he should have more powers and we have given him more powers. We have given him powers to carry out spot checks; there are new

penalties. When I first met him I asked him to tell us what he needs and we will do our best to give it.

Q1002 ***Lord Rowlands:*** To pursue individual cases where people have complained about their privacy? Is he entitled to do that?
Mr Wills: Again we need to look at future powers in the light of Walport/Thomas. These are precisely the sorts of areas that we have asked him to look at and new powers for the Information Commissioner may well be part of what they recommend. We are very concerned to support him both in terms of the powers that he has and indeed the money; he plays an invaluable role in our public life. He personally has been a consummate public servant of the highest order and so has his team; they do a wonderful job and we will support them.

Q1003 ***Lord Norton of Louth:*** Section 23 of our Data Protection Act makes provision for the appointment of data protection supervisors in each department with the role of monitoring independently the department's compliance with the provisions of the Act. That would probably fit in very much with what you were saying earlier about a change in culture within departments. The only problem is that that provision has not been brought into effect and I wondered what was the reason for that and whether there is any intention to actually move in that direction.
Mr Wills: Without wishing to evade your question too far, there is no question that we need to raise our game. As I said at the beginning technology is changing too fast, people see the opportunities too vividly and we need to raise our game; there is no question about that. How we are going to do that must depend on the result of these reviews. If I were to come before you in three or four weeks' time I might be able to discuss the policy in a little bit more detail although I suspect we will probably have to wait until the autumn for that and I would be happy to come back and do so. We set up these reviews precisely because we felt there was a pressing need to review the way Government operates. They are reporting; we have had interim reports; they are all going to be out very soon (as I said, the data handling review is out this afternoon and the rest of them are not far behind). Once we have them we will make decisions and I do not think it is a secret to say that things will have to change.

Q1004 ***Lord Morris of Aberavon:*** I would like to ask you, Minister, about the Gus O'Donnell review on the loss of personal data by a number of departments regrettably. We had the interim report and some commitments there regarding the spot checks and new sanctions. What progress has there been in implementing these commitments and completing stage two of the review?
Mr Wills: The review is being published this afternoon. The Right Honourable Ed Miliband will be standing up in the House of Commons to make a statement on this very subject. That is the progress we have made on that. In terms of implementing it, I cannot speak for all government departments in detail but we have learned lessons and continue to learn lessons from these incidents. A lot of them have come to light because departments have really realised the need to scrutinise their own procedures. These did not all happen at once; they have come to light precisely because of the reviews the departments have undertaken into the way they handle data and they have revealed, as I say, a very pressing need for change: a change in systems, change in procedures but above all this change in culture, people just have not taken the handling of data seriously enough and that has got to change. It is changing and I think if you go into departments and you talk to any permanent secretary now this is absolutely at the top of their agenda; it certainly is in our department.

Q1005 ***Baroness Quin:*** My question to a certain extent follows on from Lord Norton's question in terms of practice within Government. The Committee looked at practice in Canada as part of the inquiry and the Department of Justice there had quite a strong role in examining other departments' proposals for new data sharing provisions. I think they had departmental Department of Justice lawyers in each department reporting back to the Department of Justice itself. This may also be the kind of issue that the review is looking at, I do not know, but does the Ministry of Justice at the moment have any analogous role to this? If not, what do you think about the idea about having all data sharing proposals vetted by one particular government office with appropriate expertise and therefore ensuring a greater degree of compliance and conformity across the system and meeting the goal of joined-up Government once again?
Mr Wills: In terms of data protection it does happen pretty much like that. There is an analogous role here because Belinda and her team do provide that advice and support for data protection. There is not that role for data sharing at the moment. Again—I am sorry to keep resorting back to the reviews—clearly there is a case for that and in practice what has happened on an ad hoc basis in relation to three particular policy areas that I can think of Belinda and her team have actually been extremely helpful to other Whitehall departments in formulating data sharing proposals and trying to finesse the perception that data protection prevents as a matter of principle data sharing. Of course it does not, but there is a cultural change that needs to happen there. In terms

of data protection it happens already in effect; in terms of data sharing it is happening on an ad hoc basis but driven very much on a personal level. There is no institutional mechanism and, as I say, since I have been in this job there have been three examples where Belinda and her team have worked extremely hard to help other officials deliver a public policy objective which depended on data sharing. Free school meals was one of them, there have been two more recent ones, but it has been personal rather than institutional. I think the whole burden of what I have been saying and the burden indeed of the reason why set up Walport/Thomas was to look at how we could do these things better, more systemically and systematically. I would be surprised if there is not movement on this in the next few months, on the data sharing part of it I am referring to specifically.

Lord Peston: I am lost again; it is obviously my morning. I cannot work out what happened to Lord Smith's question because within what I thought he was going to ask I was going to ask about data sharing in the private sector.

Chairman: Lord Smith thought that the material had already been covered.

Q1006 ***Lord Peston:*** Can I ask then whether you have a view on access to private sector data? To go back to something you said earlier, if the Inland Revenue could share data with the leading supermarkets they could easily check consumption and expenditure against declared income and come very close to discovering whether you were fiddling your income tax. I take it nothing like that takes place.

Mr Wills: No. I come, as you see, with a very large file. I did read it and as far as I am aware there is none of this in it. If I may—and Belinda will forgive me—I will give you my instinctive response.

Q1007 ***Lord Peston:*** I am willing not to have that; you could write to us.

Mr Wills: I think it is a very important point; because it is a matter of principle I would be extremely concerned about it. The public and private sectors are completely different animals.

Q1008 ***Lord Peston:*** So there is no suggestion we are going down that path.

Mr Wills: Certainly not from me.

Chairman: Minister and Ms Crowe, can I thank you very much indeed on behalf of the Committee for joining us today and for the evidence you have given us. The Committee will now deliberate in private.

WEDNESDAY 19 NOVEMBER 2008

Present
Bledisloe, V.
Goodlad, L. (Chairman)
Lyell of Markyate, L.
Morris of Aberavon, L.
Norton of Louth, L.
Peston, L.
Quin, B.
Rodgers of Quarry Bank, L.
Smith of Clifton, L.

Letter from Vernon Coaker MP, Minister of State, Home Office

Thank you for your letter of 9 October in relation to your ongoing inquiry on the constitutional implications of the collection and use of surveillance and other personal data by the State. You asked for clarification on two points.

Local Authorities' Powers under the Regulation of Investigatory Powers Act 2000

When the Regulation of Investigatory Powers Act 2000, (RIPA), was going through its Parliamentary passage, local authorities were not included in the list of public authorities that could have access to communications data. Provision was made for an order making power that would enable other public authorities and additional purposes to be added. The making of an order requires affirmative resolution in both Houses of Parliament.

During the passage of the Bill there was a debate on why the order making power was required and in an exchange of correspondence the then Minister of State, Charles Clarke, confirmed that there was no intention to extend the provisions in RIPA to enable local authorities access to communications data. This was because a number of public authorities, including local authorities, already had access to communications data either by arguing individual exemptions under the Data Protection Act 1998 or by other statutory powers such as Production Orders under the Police and Criminal Evidence Act (PACE), and various other pieces of legislation including the later Social Security Fraud Act 2001. When reviewing the use of communications data it was decided that a more consistent approach was needed to ensure that proper consideration was given to necessity and proportionality.

A consultation exercise "Access to Communications Data—respecting privacy and protecting the public from Crime" was launched in March 2003. The consultation document is still available on the Home Office website on the following link http//www.homeoffice.gov.uk/documents/coms-data-2003/. This consultation document clearly sets out the issues and proposals for the inclusion of other public authorities, including local authorities, in the list of authorities that could access communications data through RIPA. It became clear that a more systematic approach was required that ensured public authorities were subjected to the same regime and to ensure a more consistent and accountable approach to all aspects including authorisations, consideration of necessity and proportionality, independent oversight and appeals mechanisms.

Following the consultation exercise an order was laid before Parliament (Statutory Instrument 2003 No. 3172 "The Regulation of Investigatory Powers (Communication Data) Order") and passed by affirmative resolution in both Houses. The order came into effect on 5 January 2004 and gave a number of additional public authorities, including local authorities, access to communications data within the RIPA regime. In the case of local authorities, this access is limited to subscriber data and billing data. Local authorities cannot access the more sensitive traffic data nor can they have access to the content of communication.

Communications Data Database

Your second point relates to the recent media coverage of "alleged plans to create a centralised database which will place a 'live tap' on every electronic communication in Britain". As you will be aware, the Government's draft legislative programme published on 14 May set out plans for a new Communications Data Bill. I think it is important to make clear that whilst we are looking at ways of retaining communications data in the future, this does not include the content of the communications, as the phrase "live-tap" implies.

Our ability lawfully to intercept communications and obtain communications data (CD) is critical to combating the threat proposed by terrorism and in tackling serious and organised crime. This includes counter-terrorism work as well as cases of child sex abuse, kidnap, murder and drug-related crime.

Communications data is used to support lawful interception by providing the key identifiers (such as telephone numbers) that are necessary to target interception correctly, and in a proportionate way. There are also other important uses of communications data; it has significant value as intelligence in and of itself, and it is used as evidence in criminal trials. You may recall the recent trial of Levi Bellfield for the murder of Amelie Delagrange. In this trial it was the use of communications data, from tracking the location of Mr Bellfield when he was using his mobile telephone, which tied him to the location and time of the murder.

However, the way we are communicating with one another is changing rapidly, with a much greater reliance on Internet-based forms of communications like email, instant messaging, social networking sites and Voice Over Internet Protocol (VOIP). There was already been a big increase in the take-up of internet-based communications. This trend will continue to grow as the UK's major providers of communications networks move toward more internet-based methods of communications, with internet protocol networks being rolled out across the country.

These changes pose significant challenges; it has been assessed that if we take no pre-emptive action, our capability to intercept communications will fall drastically from the coverage available today. Similarly, our ability to paint a persuasive picture about a subject's whereabouts and actions from communications data will be severely decreased, due to the fragmentation of data caused by internet protocols being used in core communications networks, and the proliferation of services (including third party and international services) where data will be harder to obtain or may not be obtainable at all. Without access to information provided by lawful intercept and CD, the law enforcement and security agencies' capabilities in terms of protecting national security, counter-terrorism and preventing crime will be severely affected.

A cross-Government programme led by the Home Office has been set up to maintain our interception and CD capabilities during this time of great technological change. This aims to ensure that law enforcement, intelligence and security agencies will still have access to the same vital information that they use today in order to prevent terrorism and to tackle all forms of crime.

You will be aware that the Home Secretary announced during her speech to the Institute for Public Policy Research on 15 October that the Government will be consulting on proposals in this area. The consultation will focus on explaining what communications data is and how it is currently accessed; what it is used for; the changing technology environment and the options we are considering to counteract the changes in technology and the safeguards that will apply to any new proposals.

Our intention is that we take this opportunity to listen to the public and understand their concerns and views on this. We will then look at options for legislation. Any proposals that are bought forward as a result will be published in draft for consideration before being introduced—thereby ensuring that the very valuable scrutiny which we had planned for any legislation is this area can still be achieved.

October 2008

Examination of Witnesses

Witnesses: Mr Vernon Coaker, a Member of the House of Commons, Minister of State for Policing, Crime and Security, Mr Tim Hayward, Acting Director of the intercept modernisation programme, and Mr Stephen Webb, Acting Director of policing policy and operations, Home Office, examined.

Q1009 ***Chairman:*** Good morning. May I welcome to the Committee the Minister of State for Security, Counter-terrorism, Crime and Policing, Vernon Coaker, and his accompanying officials, Stephen Webb, the Acting Director of policing policy and operations, and Tim Hayward, the Director of the intercept modernisation programme. We are being sound recorded and televised and may I ask Mr Coaker, Mr Webb and Mr Hayward please to formally identify themselves for the record, whereafter, if Mr Coaker wishes to make a short introductory statement, that would be welcome. If not, we will proceed with questions. Mr Coaker?

Mr Coaker: Thank you very much, my Lord Chairman, and good morning to you and to the rest of the Committee. Thank you very much for inviting us. My name is Vernon Coaker, Home Office Minister of State for Crime, Policing, Counter-terrorism and Security.

Mr Hayward: My name is Tim Hayward. I am the Director of the intercept modernisation programme.

Mr Webb: Good morning. My name is Stephen Webb and I am the Acting Director of policing policy and operations in the Home Office.

Mr Coaker: Perhaps I may open with a couple of sentences because I know there are a number of questions that people wish to ask and no doubt some supplementaries but we welcome that opportunity. Can I thank the Committee for the opportunity to come again to speak to you about the matters on the agenda and to explain some of the thinking that we have, some of the policies that we are pursuing and some of the issues that we are weighing up in taking forward this whole agenda. We look forward very

much to reading the report that comes out at the end of your inquiry and using that to inform our deliberations and our thoughts. I do not really want to say very much more than that, just that we very much welcome the Committee's inquiry. I have already read some of the deliberations of the Committee and I look forward to reading the full report when that comes out in due course.

Q1010 ***Chairman:*** Thank you very much indeed, Minister. Can I begin by asking if there are any core principles that you think should underpin the Government's approach to surveillance and data collection, and who in the Government is responsible for ensuring that these principles are adhered to?
Mr Coaker: Can I say that at the core of what we are trying to do is to ensure that we balance a number of particular principles. The first core principle has to be, of course, respect for human rights, the necessity to see that as an important issue with respect to all of the work that we do in this area. We have to cherish the right to privacy. That is fundamental to all of us and needs to be protected. The Government has always been clear that where surveillance or data protection impacts on privacy that should only be done where it is both necessary and proportionate. That is why we introduced the Regulation of Investigatory Powers Act 2000. It was to try and regulate the way in which these data were collected and brought in and regulate the use of surveillance and data collection by public authorities and make sure that was done with proper respect for human rights. Of course, the other principle to balance up with all of that is the desire to protect the public. Public protection obviously has to be an important part of what we are doing and surveillance and data collection are an essential and vital part of our trying to ensure that we protect the public not only from terrorism but also from serious crime. I am sure that this will be a theme throughout the morning and no doubt throughout much of your discussion. It is wrong to say we have people who are not interested in tackling terrorism and serious crime and therefore are opposed to this. It is about where we draw the line and how we have the correct balance between these things which is absolutely essential. It is not always easy to do that. There are judgments to be made and debates to be had and sometimes these threats change, as also sometimes does technology. One of the issues that we are grappling with is technology advances, technology changes, so that also puts increasing demands upon us. In terms of overall responsibility within government for taking this forward, I have the responsibility with respect to that, and I obviously meet with other ministers in a way that is appropriate and necessary.

Lord Morris of Aberavon: Thank you very much for your letter of 21 October explaining the Government's change of heart with regard to the use of the RIPA. I am old-fashioned enough to believe, Minister, that when a categorical assurance is given by a minister to a backbench MP in the course of the passage of a Bill the Government's word is its bond and it should be adhered to and, while I note your explanation, it seems to me that, although you say that you want a more consistent and more systematic approach, the ragbag of existing powers seems now, under the process of making it systematic, to be for a different purpose than was envisaged when the RIPA was being introduced and the categorical assurances were given by Charles Clarke to William Cash. It could never have been intended, could it, when the Act was brought in that local authorities would be able to use these powers to survey catchment areas for schools or for checking dustbins or the like? Indeed, some of the witnesses we have had were positively enjoying the new powers which they have.

Q1011 ***Chairman:*** Perhaps for the benefit of those who are less familiar with the subject I should interject that the RIPA means the Regulation of Investigatory Powers Act passed in 2000.
Mr Coaker: Thank you, my Lord Chairman. In answer to Lord Morris, obviously the assurance was given by Charles Clarke as the Bill went through Parliament and that assurance was given in good faith, but I think what happened afterwards, and I will deal with the other point about the use of the power if that is okay with you, my Lord Chairman, as a separate point, was that it seemed to us there was a particular problem with the fact that local authorities were already able to try and apply for access to communications data. The internet service providers were therefore having people coming to them under RIPA legislation and people coming to them under different legislation, so there was an inconsistency there. The Government then went out to public consultation about the issue that had arisen, and as a consequence of that, as you know, felt that it was only appropriate to extend the list of public authorities which were able to have access to RIPA powers, and that was then made subject to affirmative resolution in Parliament. I am afraid I cannot add any more to the explanation that that was the way to deal with this which was felt to be appropriate. On the second part of Lord Morris's question, I think there are some concerns about the way in which local authorities have used powers under the RIPA legislation, including the examples that you used, and that is why I have been talking to my colleague in DCLG, John Healey, about what we need to do about that, because we do not want to see legislation that is available for local authorities to use with respect to serious crime being used in the ways

that you have indicated and also in other ways, for example, with respect to dog fouling. Certainly that is something we need to address.

Q1012 ***Lord Morris of Aberavon:*** Minister, your explanation seems to be a bit thin because if that was in the mind of the Home Office before Charles Clarke was allowed to send his letter it might have been qualified at that stage. Why the change of heart?
Mr Coaker: As I say, the change of heart came because of a recognition of the problem that arose about the inconsistency of approach that was taking place. Some people were approaching internet service providers through RIPA legislation; others, like local authorities, were approaching them to get exactly the same information that they get under RIPA through other legislation, through the Data Protection Act, some of the exemptions that exist there, or through production orders under PACE. The debate then became that if they were doing that and we wanted to regulate in a way that I was trying to say in answer to the Chairman's question, to try to ensure that it was done proportionately, consistently, with regard to the human rights aspects that are enshrined within RIPA, that is why we then went out to public consultation to say, "Look: this is the situation. Would it not be better to include local authorities therefore within that?", and that decision was then taken and made subject to the affirmative resolution procedure in Parliament.

Q1013 ***Lord Morris of Aberavon:*** Are they getting no more under RIPA than they had already? Is that absolutely right?
Mr Coaker: My understanding is that they had access to the powers that would have been available.

Q1014 ***Lord Morris of Aberavon:*** All of them?
Mr Coaker: I think that is right.

Q1015 ***Lord Morris of Aberavon:*** If not perhaps you will write to the Committee.
Mr Coaker: Of course. Let me just say that if I am factually inaccurate on anything I will, of course, write to the Committee, and if at any time anybody feels that they need more information I will send that information to the Committee. That would only be right and appropriate. As for Lord Morris's point, I will check to make sure that that is factually right, but my belief is that that is the case.

Q1016 ***Lord Smith of Clifton:*** Might I ask the Minister if he is saying that the categorical assurance given by Charles Clarke earlier now has no validity?
Mr Coaker: I am not saying it did not have any validity. I am saying that what happened afterwards was that there were problems with the way in which it was operated, there were inconsistencies in the way that it was operating, and therefore the Government at the time, and we are talking about 2003, took the view that it needed to try and regularise that position particularly with respect to local authorities. Just to be clear in supplementing what I said to Lord Morris, my Lord Chairman, of course we are talking about communications data here. It was necessary to change the framework within which local authorities were already operating.

Q1017 ***Lord Smith of Clifton:*** Is this not a very unfortunate precedent, Minister?
Mr Coaker: I think it is fair to say that governments often are faced with difficult situations after Bills are passed. I do not think this is something that you would want to repeat. Clearly, if an assurance has been given you like to try and ensure that that assurance is maintained, but I also think, to be frank, my Lord Chairman, that sometimes there are things that happen two, three, four, five, six years later—

Q1018 ***Lord Smith of Clifton:*** Stuff happens?
Mr Coaker: I think so, my Lord. Sometimes something happens and although it is difficult you do have to say that circumstances have changed or that there is a fresh way of looking at it and despite the assurance that was made there is a need to change, and that is why we did what we did.

Q1019 ***Lord Peston:*** Minister, I thought your answer to the Chairman's opening question was cogent and convincing in the context of serious crime and terrorism and I think that would be the public view of the matter as well, but, in regard to Lord Morris's question, if we then say the same powers are being used for local authorities searching my dustbin is not the danger that you lose public support because they say the Government does not know what it is doing, and then you lose support for the area in which you most need public support, namely, the anti-terrorism, anti-crime thing? Although I personally am totally in favour of what you said, if I got into trouble with my local authority because I had put the wrong thing into a dustbin you would lose me totally. I would say if that can happen I want the whole thing stopped. I appreciate all your arguments other than that must not happen. Does the Government not have any powers just to say, as used to happen before human rights came on board, "Just do not do it", to the local authorities?
Mr Coaker: Can I say to Lord Peston that I absolutely agree with the point that he has made? I am sorry if I did not explain myself as cogently in the second answer as I did in the first. What I was trying to say in answer to Lord Morris was, of course, that if powers are used inappropriately that tempers the view. It causes people then to look at the way the whole of the legislation is used and undermines

support for it. What I was trying to say was that in terms of the examples that Lord Morris gave and the other examples that are used, things like dog fouling, they are inappropriate, and when my predecessor came in he mentioned that he thought that was inappropriate. Speaking to colleagues in DCLG, and we are looking at what we need to do to ensure that the powers are used appropriately and in a way which commands the respect of the public, I think Lord Peston is absolutely right because I think that when people understand that local authorities are actually using them for the sorts of things that people would want to see them using the powers for, therefore we have to stop some of these other things happening which undermine that support. If I can give you one example (I have got about five) so that I do not take up too much of the Committee's time but I do think it is an important one, the North Yorkshire County Council used directed surveillance and communications data authorised by RIPA to prosecute three roofers who had persuaded 11 elderly victims to pay for unnecessary work on their roofs. These victims lost in excess of £150,000, two of the 11 victims lost their entire life savings, and the three criminals responsible were sentenced to between three, five and six years. I think Lord Peston is right because we do not get the other aspects of that right in the point that Lord Morris was making and we then undermine the support which means also local authorities can use the power to tackle serious criminals like the ones in the example I have just given.

Q1020 ***Lord Lyell of Markyate:*** What you are saying is very helpful but, pinning it down, there really is no reason why local authorities should have the right to use these powers at all unless they have some function in serious or organised crime or in relation to terrorism. There is no reason why they should have the right, for example, as we have been saying, in terms of dustbins, dog fouling, school catchment areas. Would you agree with that?
Mr Coaker: In respect of dog fouling and bins I would have to agree with that, and that is the sort of area we need to look at. The reason I slightly hesitate about bins is that I could make an example up where fly tipping was a serious crime and so I do not want to get into all rubbish being something local authorities should not look into. You could make up an example of big tipper lorries going somewhere and dumping waste. I know that is not what you mean, my Lord, but do you see the point I am making? However, I do think we have to get away from this use in those sorts of ways that Lord Morris and Lord Peston have raised so that we can keep support for the other matters.

Q1021 ***Lord Lyell of Markyate:*** I agree; you have to stick to serious crime. It may be something which has to have at least a two-year prison sentence available for it—that may not be the exact test but something like that—but these other more administrative things like dustbins as opposed to serious fly tipping are in a different league. Your letter of the 21st October is a helpful letter, but whilst at the start it deals with serious and organised crime and terrorism, when you get to the third to last paragraph it says, "to tackle all forms of crime", which would include messing about with a dustbin. I think that needs to be taken on board by the Government and changed.
Mr Coaker: In retrospect "all forms of crime" I might have qualified if I were writing the letter again, but hopefully from the evidence I have given the Committee this morning the understanding is that the other ways it has been used we would regard as inappropriate and we need to ensure that it is used appropriately and we are working with DCLG on that. As I say, I have already talked to my colleague, John Healey, about how we take that forward.
Lord Lyell of Markyate: The way it should be taken forward is that the power should be restricted. It should not be a question of individual judgment by a local authority official as to whether it is necessary and proportionate. That is not good enough.

Q1022 ***Lord Morris of Aberavon:*** If I understood your North Yorkshire example correctly, there is a sound moral case for North Yorkshire doing what they have done, but surely the existing powers under the law are more than adequate. I have been involved—involved professionally, if I may say so—in cases where travellers have got gullible old people to pay £5,000 for repairing roofs and the law of the land caters for that already. There have been discussions, I understand, between Sir Simon Milton and the Surveillance Commission about the misuse of local authority powers in trivial matters. What has come out of them?
Mr Coaker: What has come out of them is the point that I have just made, that certainly myself and DCLG are now talking about how we take all of this forward and turn some of the words that we have been saying about dealing with this into action. I know Sir Simon wrote to local authorities and said to them that when they used these powers they had to make sure they were used in a necessary and proportionate way and reminded them that that is in the guidance and that is what they should be doing. Going back to the roofers very quickly, the point I was trying to make was that the use of the powers available under RIPA enabled the local authority to identify them and collect the evidence through communications data which then enabled them to be prosecuted.

Q1023 ***Viscount Bledisloe:*** Minister, as I understand it, you are now saying that the local authorities had the power to collect this data without RIPA but that it was inconvenient that they had varying powers in different directions. Your letter says that Charles Clarke confirmed that there was no intention to extend the provisions in RIPA to enable local authorities to have access to communications data. I confess I read that as meaning that they did not have that access and were not to get it. Which are you saying?
Mr Coaker: What I am saying is that, obviously, when the RIPA legislation was going through there was no intention to give them powers under RIPA but what became apparent was that they were already going to internet service providers to ask for communications data on a limited basis, but nonetheless on the basis of powers that existed under other Acts like the Data Protection Act or production orders under PACE. Following the passage of RIPA, where there were people going to the internet service providers asking for communications data under RIPA, what we thought, in the light of how it was working, was would it not be better to bring everybody under one piece of legislation so that the internet service providers knew in what context they were being asked for that information and also because we thought that because we have tried to make RIPA, difficult though it is, human rights compliant, that would be beneficial to that. That was the judgment that was made after that. We went out to public consultation and then we brought it through Parliament.

Q1024 ***Lord Morris of Aberavon:*** Are you saying that when Charles Clarke gave his confirmation he did not realise that there were these powers under the other Acts or are you saying that his answer was disingenuous?
Mr Coaker: No, it certainly was not disingenuous.

Q1025 ***Lord Morris of Aberavon:*** So he did not realise they had the powers under these other Acts but then that information came up later after RIPA had been passed?
Mr Coaker: Certainly I sometimes make decisions and try to assure people about certain things and then a year or two later, despite the assurances, it has not quite worked in the way that I expected it to. I think the appropriate thing then is to make a judgment about saying how do we address this, consulting people, explaining what the issue is that has arisen, and then bring it through Parliament and say, "The belief of the Government following public consultation, following the way it has worked, is that there is the need for us to adapt and change and amend the legislation accordingly".

Q1026 ***Baroness Quin:*** As Lord Peston said, you gave an opening statement which was strong in terms of referring to human rights and the right to privacy and the need to be proportionate. Do you feel that someone is taking overall responsibility in government for ensuring that these principles are adhered to, and how within government, given the challenges of changing technology and the ease now with which data security can be breached with lapses of data security that we have seen, and also in a situation where government outsources data collection, sometimes not even within the UK but abroad, are these principles going to be adhered to?
Mr Coaker: The overriding principle, of course, is that now because of the Human Rights Act incorporated into British law there has to be a statement in front of every piece of legislation about the legislation being human rights compliant. I think that is an important statement of principle. In terms of the responsibility for necessity and proportionality in this area of work, that will ultimately be my responsibility and I take this responsibility extremely seriously just a few weeks into the post. We meet regularly with other departments in terms of security, in terms of many of the issues that we have here, and alongside that there are the responsibilities of all the various commissioners that have been put in place for them to ensure as well that all of these processes are working properly. In fairness to your question, obviously there have been some issues with regard to data retention, and I think it is extremely important for us to continue to build trust so that when the Government holds information, when the Government has data, it ensures that that data is protected and secure. For example, the Cabinet Secretary has been working to try to bring forward new procedures with respect to that so that each individual department now looks at the way it deals with information, the way it holds information and the way it treats information. That is starting to give us a much more powerful message about the way we collect and maintain the information and data that we have.

Q1027 ***Baroness Quin:*** This also applies to outsourcing, does it?
Mr Coaker: It certainly does and in terms of memoranda of understanding and the work of the commissioners we are trying to ensure that that data and the sharing of that data are appropriate and proportionate as well.

Q1028 ***Lord Morris of Aberavon:*** Minister, am I right in thinking, and correct me, please, if I am wrong, that nothing much has flowed from the talks with Sir Simon Milton on the issue of triviality and the misuse of powers? Have you any intention of doing anything practical like a code of conduct or

guidance to local authorities or guidance in particular as to how they exercise their judgment in proportionality, which is not easy?
Mr Coaker: Let me say this, my Lord Chairman. I think it might be a good idea if I offered to come back to this Committee in the summer maybe to see what progress we have made with respect to all of this if that is helpful to the Committee. It is an extremely important area of work and I want to ensure that we have pace and momentum in taking all of this forward. If that is helpful to your Committee, my Lord Chairman, and agreeable to yourself I just leave that on the table for the Committee to consider.

Q1029 ***Chairman:*** Thank you very much, Minister.
Mr Coaker: Just on the point that Lord Morris has made, there has been some progress with respect to all this but we are now at a position with DCLG where we need to look at the codes of conduct and see how we take them forward, as I was trying to intimate, having had discussions, to ensure that we avoid some of the issues that have arisen in the past to maintain the confidence that Lord Peston was talking about in the more general use of these powers to prevent and tackle and detect serious crime and indeed terrorism.

Q1030 ***Lord Norton of Louth:*** I have two questions deriving from what you have already covered, first on the RIPA point. The criticism made is that it has been used for purposes that it was not intended to be used for, but, as I understand your point, nonetheless it may be used in a way where the effects are beneficial, and there was an example you gave. Would that possibly then be an argument for having separate legislation where something is not covered by extant legislation in order to maintain the integrity of RIPA for the purposes that it was intended for? If you had separate legislation it would allow it to be more tightly drawn to cover the sorts of examples you are talking about.
Mr Coaker: You could do that but the really important point is that I think we can do it under RIPA if we get this right. We have got primary legislation there, we have got codes of conduct which flow from that, and I think the task for us is to ensure that what we have got works rather than saying that we will have another piece of primary legislation. That would be my approach and I do not think that it is impossible for us to go forward in that way. As Lord Morris was saying, there has been a lot of discussion about this. We are now at a point where we can look forward to taking some action with our colleagues across government and, as I say, particularly with DCLG.

Q1031 ***Lord Norton of Louth:*** In a way that leads to the next question which you have already been asked about, guidance in trying to achieve that distinction so that it does not lose public support for the purposes for which it was intended. My second question follows on from Baroness Quin's about what happens within government. You mentioned that you have prime responsibility and co-ordinate and have meetings. Can I push you a bit further on that in terms of how proactive that role is, how it is best being responded to, or is there guidance given within government to ensure that the principles you have detailed are applied consistently through government?
Mr Coaker: I think up till now it has worked fairly well in the sense that I talked about. As the work develops as all of this agenda moves forward and we try and tackle some of the issues that we will no doubt come on to later, my Lord Chairman, there may be a need for us to look at how we more effectively co-ordinate action across government. Sometimes you see this as criticism. I just think it is an evolutionary process. I think if you looked back five years you might say, "What we should have done was so-and-so", so as the process evolves, as legislation evolves, as technology changes, so the response of government should be, "Have we got all the appropriate systems in place?" Officials meet regularly across government. We meet, particularly with respect to security, very regularly as ministers. As I have said, I meet with DCLG colleagues. There is sometimes a need to consider whether we need to formalise that more than we do at present.

Q1032 ***Lord Rodgers of Quarry Bank:*** With respect, would you say something a little more clear about the process of government? You talk about one minister to another. Is there a committee? Is there a way in which all legislation is examined by a minister of state of your department? How does it actually work? For example, it is not a direct comparison in any way at all but, as we all know, in government any legislation, any proposals, are always looked at by the Treasury; that is a well established convention or approach, but is there now some convention of that kind—and again, with great respect, ministers of state have very important roles nowadays but in the end it is the secretary of state, whoever it might be, who carries most weight—that it is carried from the head of the department to all members of the Cabinet? It is the process I am interested in.
Mr Coaker: There are, as Lord Rodgers will know, a number of Cabinet committees and all of these cross-government bodies that meet. What I was trying to say in answer to Lord Norton's point is that I think there is a need for us to look at how we more effectively co-ordinate at a ministerial level—

Q1033 ***Lord Rodgers of Quarry Bank:*** How is it now? You say it should be different but how is it now?
Mr Coaker: As it stands at the moment I talk to colleagues at DCLG with respect to these matters in the way that I have indicated in terms of local authority powers, in terms of how the legislation works. If we talk about security, there is a regular meeting each week with officials and ministers from across government to discuss all of that with respect to terrorist related offences. As I say, with the increasing importance of all of this area of work—the intercept modernisation programme that is taking place, some of the debate and discussion around RIPA, all of these other areas—there is a need for us to make that process more formal than it is at the present time, and I think there will then frankly be a more satisfactory answer to the point that you are making about the need for us to effectively co-ordinate across government. As I say, that is where we are at the moment and where we need to get to and we will.
Mr Webb: Can I just add something on the legislation? When we are talking about legislation we need a secretary of state's certificate of compatibility with the Human Rights Act and that is obviously something that will need to be agreed with the law officers, so there is a process there. When it comes to individual actions, again, the Human Rights Act enables people to challenge any public authority if they believe their actions are not compatible with the principles of the Act, so there are a number of processes which are already set out in law.

Q1034 ***Lord Smith of Clifton:*** Minister, we have talked a lot about trust and we all agree on the need for maintaining public trust. Does the Home Office undertake opinion polling from time to time to see what public attitudes are towards RIPA and surveillance generally? How do you make yourself aware of what the public trust is?
Mr Coaker: We have not but we are going to do some polling with respect to the popularity of all of this work, so that is the factual statement. If the supplementary to that is do I think surveillance and data collection are something which are generally supported, I think that providing it is proportionate people see it as necessary. It is a bit circular but I think it is the truth that people do support the use of surveillance and data collection techniques as long as they have that trust and it is proportionate and the work that is done is necessary, which goes back to the earlier discussion.

Q1035 ***Lord Smith of Clifton:*** There is a difference, of course, between surveillance on the one hand and data gathering on the other.
Mr Coaker: Absolutely.

Q1036 ***Lord Smith of Clifton:*** One would have to distinguish what the public's mind was between these two things.
Mr Coaker: If we look at the communications data point that we made, obviously, the threshold for agreement to that is much lower than when you start getting into the more covert, intrusive surveillance where the threshold is completely different. I think people generally understand that the need for intercept and some of the covert surveillance, some of the more intrusive powers, can only be done at a very high threshold with secretary of state approval. I think people generally understand that because they know that is associated with terrorism and very serious crime. With communications data there obviously is a lower threshold for having agreement to do that, and stop me if I get boring with this, but I do think that people generally support the use, even at a local authority level, of techniques to get communications data providing we do not have the sorts of problems that we have seen where people have seen it used for dog fouling. If it is used for the example that I gave of the roofer, and I do not want to repeat that here or go through some of the other examples that I have, I think people find that acceptable.

Q1037 ***Lord Smith of Clifton:*** Might I ask, Minister, when you are proposing to do this poll?
Mr Coaker: In the near future, as I understand it.

Q1038 ***Lord Smith of Clifton:*** "The near future" is what? Within the next six months?
Mr Coaker: If you have me back you will be able to say, "Have you done that, Minister?".

Q1039 ***Lord Smith of Clifton:*** The real problem that the Government have, and I appreciate this, is that when things are undertaken reasons of state are always prayed in aid, which is always a very dodgy ground because, as you said in your opening statement, where do you draw the line on this? That is why I would urge you to do opinion polling on a fairly regular basis, frankly, to see whether you are taking the public with you or not.
Mr Coaker: Can I just say, Lord Smith, that I have given a clear undertaking that we will do some work with respect to this to find out where we are or are not with the public, and in due course if you do not have me back I will write to you anyway.

Q1040 ***Lord Lyell of Markyate:*** You are talking about a proposed Communications Data Bill and there already exist the requirements of the European Data Retention Directive. I got the impression from your last answer that the Communications Data Bill

was somehow going to give local authorities a lot of rights to look and see what telephone calls people have made even if they could not hear the content, and so on. What are you proposing and why?
Mr Coaker: In terms of the Communications Data Bill?

Q1041 ***Lord Lyell of Markyate:*** Yes, with particular relevance to anything other than serious crime or terrorism.
Mr Coaker: As you know, as far as the Communications Data Bill is concerned it is now a proposed Bill, and as the Committee will know we are concerned about the way in which the capacity of law enforcement and the security services to access some of the data that they have been able to access is diminishing and we are concerned about some of the threats there are to that. It has been well publicised by senior police officers, by the Director General of the Serious and Organised Crime Agency and some security services that they are concerned about the changes to the way in which we are communicating. Frankly, Chairman, the problem is that in a technological world where all of us are struggling to keep up the idea that all of the communications can be accessed now because somebody phones somebody else and the way in which it is changing through the internet is problematic for us. As a Government we have to take account of those changes in technology to ensure that our law enforcement and security services have the capacity to collect the information and data that they need according to and consistent with the principles that I laid out at the beginning. Where we are the present time is that we are looking at the options that are available to us and we will publish those options in the new year, January/February, for public consultation.

Q1042 ***Chairman:*** As a Green Paper?
Mr Coaker: As a public consultation document. All the various options then will be available for people to look at, for people to debate, discuss and come to some sorts of conclusions themselves about what they think is necessary, proportionate and appropriate.
Mr Hayward: If I could just expand on the bit about the EU DRD, at the moment under the EU DRD the telecoms companies hold business data which can then be accessed by the authorities under RIPA. The problem moving forward is that the telecommunications companies will not necessarily hold all the data for business purposes and therefore it will not be available for the authorities to access.

Q1043 ***Lord Lyell of Markyate:*** So what is going to happen?
Mr Hayward: That is why we are looking at different ways in which we can collect that data and allow that for access.

Q1044 ***Lord Lyell of Markyate:*** Has this got anything to do with local authorities? If it is MI5, MI6 and serious crime I do not think we are probably too fussed.
Mr Hayward: No. It is aimed at serious crime and the intelligence agencies.

Q1045 ***Baroness Quin:*** Lord West of Spithead answered a question in the House of Lords about this earlier this week. He said, "We are not proposing that data that have never been collected are held". Is that right? In other words, what the Government is concerned about is losing access to data that it already has, not about collecting extra data?
Mr Coaker: Baroness Quin is absolutely right, my Lord Chairman. It is about maintaining our capacity, not about increasing it.

Q1046 ***Chairman:*** Can I ask, Minister, when the consultation document is published in the new year whether there will be some quite substantial explanatory material to enable people who will want to respond to understand what it is all about?
Mr Coaker: Absolutely, Chairman. I think there is a need for us to put that out alongside the consultation document and that is why Mr Hayward is working particularly on this project. We are very keen for debate and discussion to be engaged because it really builds on some of the things that Lord Peston and Lord Norton were saying earlier on. Part of the issue here is to get the facts out there so that people can engage with the debate so that, instead of having a debate about something that may or may not happen, we have a debate about the serious options that are available. From a Government perspective if you have chief police officers, security services, the Serious and Organised Crime Agency all seriously concerned about the diminishing capacity that they face, then we need to put those options before people and say, "These are the ways that you could address it", and what is acceptable to us and what is not.

Q1047 ***Viscount Bledisloe:*** I want to ask you various questions about the national DNA database. First of all, according to the Home Office website our DNA database is the largest of any country in the world. Is that right?
Mr Coaker: I think so, yes. Proportionately it is, so yes, I guess so.

Q1048 ***Viscount Bledisloe:*** We are told that over five per cent of the UK population is on that database whereas in America it is only 0.5 per cent. Is that right?

Mr Coaker: The figure I have is that 7.39 per cent of the UK population have a profile on the DNA database.

Q1049 ***Viscount Bledisloe:*** 7.9 per cent?
Mr Coaker: 7.39 per cent of the UK population have a profile on the national DNA database.

Q1050 ***Viscount Bledisloe:*** Is it right also that last year more than 700,000 samples were added to that database which was a record increase for any one year?
Mr Coaker: I think that will be about right. The reason I hesitate slightly is that I have hundreds of statistics in front of me and it depends what month you use and they change almost daily, but certainly there would have been a significant increase.

Q1051 ***Viscount Bledisloe:*** That is what your official is there for.
Mr Webb: It sounds right.

Q1052 ***Viscount Bledisloe:*** What on earth is the justification for us having so much more of our population on the database than anybody else in the world?
Mr Coaker: Partly because it has enabled us to solve a significant number of serious crimes. If you look at the numbers of murders, rapes, serious robberies and other violent crimes that have been solved as a result of having that database, we think that in the end is a proportionate response to tackling crime and it is a justification for it.

Q1053 ***Viscount Bledisloe:*** Are you saying that America, which has only 10 per cent of what we have, or on your figures even less, only solves 10 per cent of the murders that we solve?
Mr Coaker: I do not know what the figures are as compared to America in terms of crime rates. The point I am making is that the Government's decision here and the judgment that has been made is that the DNA database and the collection of DNA samples to be put onto the DNA database have proved an extremely effective way of tackling crime.
Mr Webb: It is also worth pointing out that we started many years before other countries so our database naturally is larger because we have a longer series of entries. We were first and also we have a national system whereas in other countries they have a more federal system. It took longer to establish the idea of a national database.

Q1054 ***Viscount Bledisloe:*** Does it follow from what you are saying that you would think it desirable if the entire population's DNA was on the database?
Mr Coaker: No, I would not find that acceptable.

Q1055 ***Viscount Bledisloe:*** Why not?
Mr Coaker: Because we have taken a decision that first of all people who have been convicted of an offence have their DNA samples retained. We then changed, as you will know, through two Acts of Parliament in recent years, so that now DNA samples can be kept for people who are not only convicted or charged but now arrested and detained at a police station. I think that is the appropriate response. I think that is a response that is proportionate and I think is a response that commands the support of the population. I do not believe, certainly at the present time, that a national database of everyone is appropriate. Let me just say this. Even though there is significant debate and argument about the fact that in England and Wales we retain DNA samples from people who have been arrested but not subsequently charged, there is still a threshold there because the officer who arrests somebody has to arrest them according to the PACE procedures. That requires them to have reasonable suspicion that they have committed a crime. They also then have to be taken to a police station and the custody sergeant there has to decide that that person should be detained. There is a debate and an argument about that. Some people do not think that is a high enough threshold. I think that is an appropriate threshold. There are others who would argue for a national database. That is not where the Government is coming from on this. We think we have got it right and we think it is proportionate to us in order to help us tackle serious crime.

Q1056 ***Lord Lyell of Markyate:*** Just to help analyse that a bit, personally I am quite in favour of anybody who has got a criminal record having their DNA on the database, but when you come to people who have been just arrested or maybe charged but the charge is never proceeded with, or when they are found innocent or not found guilty, that is the area of debate, is it not? Do you have any statistics as to what number of crimes have been solved as a result of information held on the DNA database which does not relate to people who were convicted, and if you can break them down into those three categories it would be helpful?
Mr Coaker: I have got that information here. The provisions of the Criminal Justice and Police Act 2001 came into effect on 11 May 2001. Between that date and 31 December 2005, which are the latest figures we have, there were approximately 200,000 DNA profiles on the national DNA database which would previously have had to be removed before the 2001 Act was introduced because the person was acquitted or the charges were dropped. Of these 200,000 profiles approximately 8,500 profiles from

some 6,290 individuals have been linked with crime scene profiles involving nearly 14,000 offences. These include 114 murders, 55 attempted murders, 116 rapes, 68 sexual offences, 119 aggravated burglaries and 127 of the supply of controlled drugs.

Q1057 ***Lord Lyell of Markyate:*** The weasel words are "linked in", are they not? How many of those 6,290 people's DNA have led to their conviction?
Mr Coaker: I will write to Lord Lyell about that, but it certainly does demonstrate that there is a read-across from the retention of that DNA to a significant possibility that large numbers of people have been responsible for serious crime, but I will investigate that for you and write to the Committee with that figure.

Q1058 ***Chairman:*** Thank you very much indeed, Minister.
Mr Webb: It is going to be a very difficult thing to prove statistically because obviously it is going to be one item amongst a lot of other things at trial. It might want to show the DNA link, it might lead to a confession, there might be other evidence or it might have been contested. We will do our best but it is not going to be easy to come up with precise figures.

Q1059 ***Lord Lyell of Markyate:*** That is not going to be difficult. Once you have got the DNA link, if the person is convicted you can tell it. That is pretty straightforward.
Mr Coaker: It is a very important point and we will write to the Committee with that information.

Q1060 ***Lord Peston:*** Just to clarify, I think what you are talking about in economic terms would be the marginal productivity of being on the DNA database and therefore it would not be 100 per cent because no system works that way. It would be a contributory factor.
Mr Webb: Yes, and I believe these are cleared-up crimes, but we will write back to confirm.

Q1061 ***Lord Morris of Aberavon:*** Minister, since DNA has been so valuable (and I support that) in clearing up some very important high profile crimes, would it not be logical—you might get an even bigger dividend—if everyone were on the national register, as supported by eminent judges like Lord Justice Sedley and others? Secondly, what is the justification, if you do not go down that road, for innocent people being kept on the register?
Mr Coaker: The judgment that you make is about where you think the line about what is necessary and proportionate should be drawn. The Government's view at the present time is that a national DNA database, notwithstanding some of the benefits that might accrue, is not a proportionate response and is not something that would necessarily command the support of the population. We do, however, believe that where somebody has been convicted there is no debate about that: their DNA should and would need to be retained in that circumstance. Alongside that the other threshold we have is the issue with respect to somebody who has been arrested and has been through the PACE procedures and the fact that they have been detained in a police station. Obviously their DNA will be retained in those circumstances but it is important to remember that retaining somebody's DNA in those circumstances is not saying that somebody is guilty or innocent of anything. It is just a matter of retaining their DNA because you have regarded that as meeting a reasonable threshold for DNA to be retained.

Q1062 ***Lord Morris of Aberavon:*** Just because he has been in a police station?
Mr Coaker: Because he has been arrested for an offence which a police officer has to have reasonable suspicion of, because that offence has to be a recordable offence and, of course, because he has been taken to a police station where the custody sergeant believes that he should be detained while further investigations are made. That is the threshold that is met. It is not just a case of everybody having to be on it. There has to be that threshold test met.

Q1063 ***Lord Morris of Aberavon:*** Not charged?
Mr Coaker: No.

Q1064 ***Viscount Bledisloe:*** I can see the practical force of this but what you are saying amounts really to saying they would not have been arrested and locked up if it had not been that they had probably done it.
Mr Coaker: No. All I am trying to say is that police officers can only arrest somebody if they act in accordance with the PACE code, and the PACE code requires a police officer to have at least a reasonable suspicion that the person they have arrested has committed an offence. That offence has to be of the standard of a recordable offence. They then have to be taken to the police station and at the police station the custody sergeant or whoever is responsible then has to take the decision that that person should be detained.

Q1065 ***Viscount Bledisloe:*** I follow all that, but what you are saying, after it has been decided that they shall not be prosecuted or their acquittal, is, "Surely it is sensible to keep this data because they probably did it, or at least if they did not do it they probably did something very similar".
Mr Coaker: It is a proportionate response to the question, is it possible that some of the people who come into contact with the police in the way that I

have said may be people who it would be beneficial in terms of the public good for their DNA to be retained.

Q1066 ***Viscount Bledisloe:*** That is the same thing as I said but rather more mealy-mouthed.
Mr Coaker: Was it? I was not trying to be mealy-mouthed. I was trying to explain. In the end you make a judgment. There will be those, and there may be people in this Committee, who think that there should be a national DNA database. We do not believe that but we think there are certain thresholds that should be met and the debate and discussion that take place on the threshold we have set is where somebody is arrested and then detained at a police station. The debate will no doubt continue on that.

Q1067 ***Lord Lyell of Markyate:*** Moving on, the Government published something called the *National Identify Scheme Delivery Plan 2008* in which you say that "[t]here will be the strongest possible oversight of the Scheme", and that this is to be provided by a National Identity Scheme Commissioner under the 2006 Identity Cards Act. What does this really mean? How does a commissioner in millions of cases give the strongest possible oversight? Who is going to do it and how is it going to work?
Mr Coaker: We will have a National Identity Scheme Commissioner. We hope and expect that person to be in post, as I understand it, by the middle of next year. By the summer of 2009 there will be a commissioner appointed with sole responsibility to oversee the way the National Identity Register database works. The scheme commissioner will have oversight of the entire scheme, will have to report to Parliament at least once a year. If the commissioner uncovers an issue with the way the scheme is functioning or the National Identity Register works he can raise that with the Home Secretary, he can report, for example, inappropriate use or storage of information to the Information Commissioner, and the work between the identity scheme commissioner and the Information Commissioner I think will be essential. They can make a report to Parliament outside of the annual report, and, of course, if they uncover—and we hope that they would act proactively with respect to this—criminal cases they can report those to the police under various sections of the Identity Card Act. All government departments will have a statutory duty to provide whatever the commissioner and his or her staff need in order to carry out their function, so I think this will be a commissioner who will be quite a significant figure in ensuring that the register works in the way it is supposed to.

Q1068 ***Lord Lyell of Markyate:*** How many million people are going to be on this scheme over the next five years and how is this man or woman going to carry out this immense task? Are they going to wait for some mistake to happen and then look into it? What are they going to do?
Mr Coaker: No. As you know, the identity card scheme will roll out incrementally. It started with foreign nationals and will be moving to airside workers next year and then to students, so there has been an incremental roll-out of the identity card scheme, but, of course, the importance of the work of the commissioner will be not to wait for something to happen. I take your point absolutely. It is for them to be proactive in the work that they do. I cannot put an accurate figure on how many people we expect to be on the register within five years. That would be pure speculation. I do not know what the answer to that will be, but certainly we would expect the commissioner to be proactive, tough and resourceful in the way that they take this work forward.

Q1069 ***Baroness Quin:*** I want to raise the issue of CCTV where again the UK seems to be in strong contrast to many other countries in terms of the scale of cameras that we have. Obviously, the Committee recognises that often these schemes can be popular and also that the cameras themselves are not owned by one authority; there is a mixture of public and private cameras. Nonetheless, what is the Government's current thinking about CCTV? In particular, given that the National CCTV Strategy of October 2007 recommended a national body responsible for the governance use of CCTV, what has been the follow-up to that recommendation?
Mr Coaker: Can I say to Baroness Quin, my Lord Chairman, that the Government agrees with the recommendation in the National CCTV Strategy, that there should be a national body for the governance and use of CCTV in this country, and we will be looking to establish one. I cannot give a timeframe for that but when I say I cannot give a timeframe I am not saying it will be in five years' time. I am saying there will be a national body that we will establish to oversee CCTV. I think CCTV is very popular, and I take Lord Smith's point about polling evidence for that, but if I look at my own constituency where people come to see me the demand is not for less CCTV; it is always for more. Also, and I am sure this is true for members of the Committee in their own communities, people see it as a very effective safety measure. I have seen all the various debates that there are about it. All I can say is that everywhere I go and for nearly everybody that I speak to CCTV has been something which promotes public safety, helps tackle crime and is fantastically reassuring. Having said that, there are issues that arise from it and certainly I think a

national body overseeing all of the work and the roll-out of the strategy and some of the issues will be extremely helpful. I think you asked about the statutory regulation. Our view is that we want to see how the national body works and how effectively it puts in place some of the various things that are supposed to be happening already with respect to data protection and registration. It is not something that we would necessarily dismiss but in the first instance we want to establish the national body and see how that works with respect to voluntary regulation, keeping in our back pocket the need, if necessary, to do more.

Q1070 ***Baroness Quin:*** I think you said that you envisaged the national body overseeing new schemes. Would the national body also have a role, or do you think it should have a role, in terms of reviewing the utility of existing schemes?
Mr Coaker: Yes.

Q1071 ***Lord Peston:*** There are two ways of interpreting the surveillance problem. One is to say that we live in exceptional times and must accept a sacrifice of civil liberties but all that will end in due course. The other is that terrorist and serious crimes are permanent and thus the sacrifice of civil liberties must be expected. Which of those views is the correct one or is the question completely unanswerable?
Mr Coaker: I think different times require the appropriate response to that particular time. It is difficult always to say that in 50 years' time this will be the circumstance and therefore it will be completely different from now—worse, better or whatever. Times change, technology changes. There are difficulties, there are threats to us, as we know only too well, which we have seen on our streets, and that requires us to take action against them. An important point is to say this: society should respond in the appropriate way to the threat that it faces at that particular time, always having regard to the need to balance national security with human rights, and the judgment of where that line should be drawn will vary from one age to the next.

Q1072 ***Lord Peston:*** So if one tried to draw an analogy with the war when we had our identity cards, limits on travel and all that but then we won the war and we got rid of it fairly rapidly, that would be a wrong analogy to the present day?
Mr Coaker: In a time of outright war there is a more dramatic change perhaps between being at war and being at peace. What we are trying to ensure at the present time is that at a time of peace, at a time of prosperity in a democracy those who threaten us, and those threats have changed over time and may change in the future, we take action against in a way which is proportionate but does not threaten our own democratic traditions and institutions in a way which people would regard as unacceptable. As always, that is a balance and the debate takes place as to where you draw the line.

Q1073 ***Lord Morris of Aberavon:*** Minister, I am grateful for the help you have given to us in your answers. May I oversimplify it? This is a constitutional committee and although we have dwelt on the merits we are not really concerned with the merits; we are concerned with constitutional propriety. Are you content that it is not a misuse of powers for a terrorist act to be used as a tool to catch fraudulent roof tilers? Would it not be better perhaps, if there is a *lacuna* in the machinery to catch roof tilers, and I suspect there is not in my knowledge and experience, for what it is worth, to have primary legislation, The Catching of Fraudulent Roof Tilers Act?
Mr Coaker: I think the first thing to say is that although RIPA obviously can be used with respect to very serious matters—terrorism and so on—we do not see RIPA as primarily a terrorist piece of legislation. RIPA is a piece of legislation which brings together all of the various techniques with respect to surveillance, with respect to human intelligence, with respect to the collection of communications data, that are appropriate in a whole range of circumstances. I think it is important for us to say loudly and clearly that although aspects of it may be used to tackle terrorists it is not a terrorist piece of legislation.

Q1074 ***Viscount Bledisloe:*** Mr Webb suggested in relation to my questions about DNA that one of the reasons why our database is larger than anybody else's is that we started earlier than anybody else. Could you write to us setting out the way in which that works?
Mr Webb: I am told the US's is now bigger than ours in numbers.
Mr Coaker: We can again write to the Committee if that is helpful.

Q1075 ***Viscount Bledisloe:*** Yes. If the answer is that America's will be the same proportionate size as ours when they catch up that would be very useful to know.
Mr Coaker: My Lord, we will write to you again if that is helpful to you and the rest of the Committee.

Q1076 ***Chairman:*** Thank you, Minister. The final question is perhaps you could give the Committee an indication of when to expect a response to the Thomas report on data sharing which was, I understand, expected earlier this month.

Mr Coaker: I thought that was soon. My Lord Chairman, can I apologise? I do not want to finish on a sour note. I will have to write to you on that one as well. I thought it was by the end of this year but I may be misleading you by saying that. I shall write to you.

Chairman: Minister, may I, on behalf of the Committee, thank you and Mr Webb and Mr Hayward very much indeed for your attendance and for the evidence which you have given, which we shall deliberate on with immense interest.

Supplementary letter from Vernon Coaker MP

Following my oral evidence session on 19 November I undertook to write to you on a number of areas.

Regulation of Investigatory Powers Act (RIPA)

The Committee asked for confirmation that allowing local authorities to access communications data under RIPA did not enable them to obtain more than they were previously able to via other means.

I thought it would be helpful to make it absolutely clear that we were not seeking to expand the types of data that local authorities can request. Local authorities have a number of statutory enforcement functions, many of which are their sole responsibility. These include trading standards investigations, environmental health investigations, housing benefit and planning investigations, landlord/tenant harassment issues and tackling anti-social behaviour. The ability to access and disclose communications data is key to effective investigation and resolution, which in many cases may result in a prosecution.

Under RIPA local authorities can request:

— Subscriber information. For example: who owns this phone? What is their address/do you have other contact information?

— Service use information. For example: itemised call records, information about the provision and use of forwarding/redirection services.

However, they can only request this data for the purpose of prevention and detection of crime and prevention of disorder. Requests have to be properly authorised with consideration given to the necessity and proportionality of the request. Local authorities also fall within the RIPA oversight and inspection regime. This is provided by the Interception of Communications Commissioner and his staff.

Under pre-RIPA arrangements local authorities could request the same information and potentially more if they could justify it, but did so through a variety of different routes which led to inconsistency and delay. There was also no independent oversight. The number of communications data requests from local authorities has declined since they were brought within RIPA.

Perhaps it would also be helpful to clarify a couple of other general points which arose during the evidence session. Although on a number of occasions I made reference to internet service providers—requests for communications data can be made to any communications service providers.

Secondly, there is a hierarchy within RIPA so that the more intrusive powers, such as the ability to seek an interception warrant, is limited to law enforcement and intelligence agencies and for more limited purposes—ie for national security and for the prevention and detection of serious crime.

This approach also applies to communications data—for example whilst a number of public authorities, including local authorities, can access subscriber and service use data for the prevention and detection of crime and the prevention of disorder, access to the full range of communications data- including traffic data is restricted to a more limited number of public authorities. This latter group includes law enforcement and intelligence agencies, emergency services and some regulatory bodies such as the Information Commissioner's Office who have a demonstrated need for it.

Public Attitude Research

The Home Office conducts public attitude research four times a year at quarterly intervals and we publish the results annually in November. We survey 2,000 adults then weight the data to the profile of the population. We research across a range of Home Office issues; some questions remain constant and are tracked over time. However, we also allow for supplementary questions to be added informing us of public attitudes towards

topical issues. Work is already underway to assess public attitudes towards the type of information and data used for crime fighting and public protection purposes. The results will be available in the New Year and I will write to update you.

DNA

Turning to the question raised about linking matches on the National DNA Database (NDNAD) to convictions, it might be helpful if I first briefly set out how the database operates.

The NDNAD contains DNA profiles derived from samples taken from known individuals (usually persons who have been arrested for a recordable offence though there are 32,000 profiles from volunteers who have consented in writing to the retention of their DNA profiles on the NDNAD). It also holds DNA profiles collected from crime scenes, for example, saliva, blood, skin cells, or semen which are believed to have been left at the scene by the offender.

A "match" means that a profile taken from a crime scene sample matches DNA taken from an individual, giving the police a lead on the possible identity of the offender. The table below shows the number of matches arising from searching on the NDNAD. In some cases where there is a known suspect, his or her DNA may be directly compared and matched to the DNA crime scene sample in a forensic laboratory. In cases like these, there may not be a need to search the NDNAD. Such cases are not included in the figures below which therefore understate the contribution of DNA to investigating serious crime (a breakdown of the actual figures I quoted when giving evidence is not available but I hope that the following information illustrates the point).

A match provides the police with an intelligence lead on the possible identity of the offender for further investigative follow up. A "detection" means that a crime with a DNA match has been cleared up by the police. Crimes with a DNA match often also result in further detections for other offences (known as "additional" DNA detections) as a result of further investigation linked to the original offence (in other words, the detection of one offence through a DNA match may also lead to other offences being solved eg because an offender on being presented with DNA evidence linking him to one offence confesses to other offences). On average, each crime detected with DNA results in a further 0.9 crimes being detected. In 2007–08 there were 15,420 additional detections, bringing the total of DNA related detections to 33,034.

2007–08	*Crimes where scene DNA profile matches any person profile*	*Detections of Crimes with DNA matches*
Criminal Damage	5,432	3,180
Domestic Burglary	8,043	3,443
Drugs Offences	1,000	321
Homicide	363	83
Other Burglary	7,211	3,886
Other Sex Offences	163	64
Other Violent Offences	1,766	849
Rape	540	184
Robbery	1,432	617
Theft From Vehicle	3,544	2,201
Theft of Vehicle (inc unauthorised taking)	4,223	1,379
All Other Recorded Crime	3,659	1,407
Total of 12 Crime Types	**37,376**	**17,614**

To put these figures in context, in 2007–08 there were 60,134 crimes where a fingerprint match was available, 24,799 detections with a fingerprint match, and 20,690 additional detections arising from a fingerprint match.

Criminal investigation involves using leads to widen or focus the scope of an investigation and assemble different types of evidence which may be presented in a trial. If a conviction follows, it would only be possible to say that the conviction resulted from DNA by forming a view of the role of a DNA match in the investigation, and assessing the weight that DNA evidence had in relation to other types of evidence in the minds of the judge, jury or magistrates. These judgements would be difficult and subjective, so statistics are not collected on the number of convictions arising from DNA.

International Comparisons

Questions were also raised on the size of the NDNAD in comparison with DNA databases abroad. As at 30 September 2008, there were an estimated 4,632,000 individuals with records on the NDNAD submitted by all police forces, of which 4,356,000 were submitted by English and Welsh police forces. At mid-2007, the United Kingdom population was estimated at 60,975,000 (*Source*: Office for National Statistics). Comparing these two figures gives a figure of 7.6% of the UK population with a profile on the NDNAD. This figure does not take account of any increase in the UK population between mid-2007 and 30 September 2008 and is therefore likely to be a slight overstatement.

The FBI website (http://www.fbi.gov/hq/lab/codis/clickmap.htm) shows that the US National DNA Index (NDIS) contained over 6,297,000 profiles at September 2008, which is 2.06% of the estimated US population of 305,732,000 (http://www.census.gov/main/www/popclock.html).

In recent years the number on the US National DNA Index has increased much more rapidly than the number on the UK NDNAD, having risen to its present figure from 2.8 million profiles at the end of 2005. The legal position is complex because of the differences between states, but the federal DNA Fingerprint Act 2005 widened powers to take and retain DNA.

There are three reasons why the UK has a larger proportion of its population on the DNA Database than other countries:

— the UK is a pioneer in DNA technology and has had a National DNA Database since 1995, before any other country;

— under the DNA Expansion Programme, £300 million was spent between 2000 and 2005 to ensure that the police took DNA from everyone they had the power to;

— police powers to take and retain DNA are generally wider in England and Wales than elsewhere. For example, legislation providing for the taking of DNA samples in some other countries permits the taking of DNA on arrest but only permits retention if the person is subsequently convicted. As a result, they have a smaller proportion of their population on their DNA database.

Number of Profiles Added to the NDNAD Each Year

On the question about the annual increase in the size of the database, the number of subject profiles (ie profiles taken from known individuals, not from crime scenes) added to the NDNAD for English and Welsh forces in each year is shown in the following table. The numbers cannot be added to give the total number of profiles on the NDNAD, as some profiles will have been removed throughout each year (for example, because of duplicates—see below).

The number of subject profiles held on the database is not the same as the number of individuals with a profile on the database because on some occasions duplicate profiles for the same person are loaded onto the NDNAD. For example, because the person provided different names or different versions of their name on separate arrests, or because profiles are upgraded. At present 13.3% of profiles are estimated to be duplicates but this rate has changed during the history of the database.

Year	*Subject Profiles Added*
1995–96	32,999
1996–97	78,899
1997–98	123,200
1998–99	227,624
1999–2000	191,173
2000–01	373,496
2001–02	470,016
2002–03	444,427
2003–04	431,771
2004–05	480,337
2005–06	625,859
2006–07	667,747
2007–08	541,920

THOMAS REPORT ON DATA SHARING

The Government's response to the Data Sharing Review was published on 24 November. The Government believes that although the current regulatory framework does not require sweeping changes, more must be done to ensure that the Information Commissioner's Office (ICO) has the powers and resources necessary to carry out its duties under the Data Protection Act 1998 (DPA). The tools available to the ICO must be flexible enough to meet a range of circumstances and encourage good practice, allowing it to take firm and assertive action when necessary. It proposed to legislate to enable the ICO to:

(i) impose monetary penalties on data controllers for deliberate or reckless loss of data;

(ii) inspect central Government Departments and public authorities compliance with the DPA without always requiring prior consent;

(iii) require any person, where a warrant is being served, to provide information required to determine compliance with the DPA;

(iv) impose a deadline and location for the provision of information necessary to assess compliance;

(v) publish guidance on when organisations should notify the ICO breaches of the data protection principles; and

(vi) publish a statutory data sharing Code of Practice to provide practical guidance on sharing personal data.

The Government will seek to introduce relevant legislation in Parliament as soon as suitable legislative slot becomes available in the next Parliamentary session.

11 December 2008

Further supplementary letter from Vernon Coaker, MP

Thank you for you letter of 18 December. You asked whether local authorities could use directed surveillance or covert human intelligence sources prior to being able to do so under the Regulation of Investigatory Powers Act 2000 (RIPA), and, if so, what the statutory basis was for such activities.

Prior to RIPA, the use of directed surveillance or covert human intelligence sources by any public authority, including local authorities, was unregulated. There was no specific statutory basis for, or statutory prohibition on, the use of these techniques; public authorities, including local authorities, did use techniques which would now be authorised as directed surveillance and covert human intelligence sources. There was no established authorisation process, no requirement for independent oversight and no independent complaints mechanism. Conversely, public authorities had no protection in law if they used these techniques.

RIPA addressed this situation and should be seen alongside the Human Rights Act 1998. It was designed to ensure public authorities would comply with the ECHR, particularly the right to privacy in Article 8, when they used covert investigatory techniques. It did not create any techniques or give any new powers to public authorities. Instead, it regulated the use of covert investigatory techniques which were already widely used. In respect of directed surveillance and covert human intelligence sources, it did this by making provision for a rigorous authorisation process independent oversight and an independent complaints mechanism. It also gave public authorities protection in law if they used techniques under RIPA.

Local authorities were added to the list of public authorities able to use directed surveillance and covert human intelligence sources under RIPA in Statutory Instrument 2003/3171. This came into effect on 5 January 2004.

12 January 2009

Written Evidence

Memorandum by Pauline Norstrom, Group Head of Marketing, AD Group

Summary

The application of CCTV has grown dramatically in the UK in the fight against crime and terrorism. Given this it is vital that sufficient attention is given to the privacy of citizens, especially in light of the implementation of new technologies. The breaching of current legislative controls on CCTV to gather evidence—however beneficial it may at first appear—should only be allowed in exceptional circumstances such as after a terrorist attack. Attention also needs to be paid, with the advent of digital technology, to the potential for different types of information to be cross referenced and provided to third parties without the knowledge of the individuals concerned.

1. CCTV in a Changing World

When it comes to surveillance in the UK today CCTV (Closed Circuit TeleVision) is pivotal to any discussion regarding the right balance between the citizen and state and the likely impact of such measures on their privacy. The reality is that individuals are now liable to be monitored and recorded in a multitude of settings, whether it be walking through our town centres; taking cash from an ATM; shopping in a retail outlet; traveling by public transport or even in their vehicles as part of congestion charging schemes.

Given that CCTV is a technology where Britain leads the world in terms of the number of systems per head of population, it is important not just for our own citizens but others who look to us for a lead—the French for example have changed their restrictions on public space surveillance as a result of the quality of evidence which CCTV produced in the wake of the London bombings—that the way CCTV is being applied to tackle crime and terrorism pays due attention to the privacy of the individual.

2. New Solutions, New Challenges

The capability of CCTV systems has changed dramatically in recent years with the move from analogue to digital allowing more powerful and flexible systems to be rolled out for commercial and public space surveillance; the ability to record more pictures per second (driven by the development of more powerful video signal processors); cheaper storage; mobile systems on buses and trains; the increasing application of CCTV in a networked environment and new ways to automatically analyse images—from automatic number plate recognition to patterns of behaviour—and associate images with data captured elsewhere. Necessarily this rapid transformation brings with it new challenges to which legislation and industry standards must be able to respond.

There are, of course, already a number of key measures in place which impact positively on CCTV, such as the Human Rights Act 1998, the Data Protection Act 1998 and a CCTV Code of Practice produced by the Information Commissioner's Office which first appeared in 2000. These have been supplemented by the development of controlling standards in specific areas—BS8418, the Code of Practice for detector activated CCTV is a good example—and licensing of CCTV operatives that monitor cameras in public spaces through the SIA (Security Industry Authority).

Whatever the pressures from the Police or security services in the fight against crime and terrorism we need to be extremely cautious in how—if ever—we choose to breach the terms of Human Rights Act and Data Protection Act with regards to CCTV. This should only be considered in exceptional circumstances, for instance to gather evidence in the wake of a major terrorist incident, and even then any breach should be within carefully defined boundaries.

3. Privacy Masking—Keeping CCTV Focused

One area which serves to illustrate the need for users of CCTV to respect the privacy of individuals, and for effective safeguards to be in place, is so-called "Privacy Masking". Basically this refers to techniques applied to control what can and cannot be seen by a CCTV system and applies equally to images displayed in real time for surveillance purposes and images recorded for later use. An example could be windows of private dwellings within the field of view of the CCTV system.

The application of Privacy Masking in the UK has been driven by the legislation mentioned above and a CCTV Code of Practice produced by the Information Commissioner's Office which first appeared in 2000. This includes the following requirement: that equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment.

It is vital that if camera fields of view overlap surrounding spaces then measures are taken to ensure privacy. One approach is through the positioning of cameras, where this is not possible—and the camera's view still infringes a private area—then either written permission from the person who owns or resides in the space has to be obtained, or physical or electronic image masking needs to be employed.

4. Unmasking CCTV

Focusing on electronic forms of masking, typically this takes place in or close to the camera, in which case images behind the mask can never be retrieved but with advances in digital recording technology, the masks can also be within the recording device itself; allowing authorised users' access to the masked part of the image. The latter capability raises the question of who should or should not be given access to the masked images. Where a terrorist attack occurs there may be a legitimate case for requiring organisations adjacent to the event to give Police officers access to masked footage if this covers an area pertinent to an investigation with valuable evidence likely to be retrieved.

Masked images of areas outside a specific scheme should not be made routinely available to law enforcement or Governmental agencies as such a move has the potential to undermine the rationale for implementing privacy masking in the first place and raise genuine concerns amongst private citizens adjacent to schemes.

It is also critical that the integrity of the privacy masking system is maintained, with its configuration protected to prevent settings being altered, bypassed or overridden by unauthorized persons.

The BSIA (British Security Industry Association) has produced guidance in this area which can be downloaded at www.bsia.co.uk/publications.

5. Chip and PIN—An Opportunity and Threat

The rolling out of the high profile chip and PIN initiative—launched in February 2006—to combat credit and debit card fraud in the UK serves to underline the need for vigilance when integrating different surveillance technologies to ensure that the protection afforded to an individual by one measure is not undermined by the ill considered use of another.

There are a number of issues which need to be addressed regarding the use of CCTV in the context of the successful operation of Chip and PIN; specifically the positioning of Chip and PIN terminals both static and mobile; CCTV at the point of sale, particularly the location of fixed cameras, so PIN information cannot be clearly identified; how cameras used for transaction monitoring should be handled and, crucially, to ensure that the pre-set positions of moveable cameras are not going to capture a customer's PIN information.

In the event that CCTV systems are integrated with an EPOS (Electronic Point of Sale) system to record CCTV data associated with a transaction it is also imperative that PIN data is excluded.

6. Information Control

With the growing sophistication of CCTV—and the potential to cross-reference images with other data—legislators need to be wary of connections being made between such information—through processes such as data mining—and questions need to be asked about where both the ownership of such data and the consent for its use actually lies.

Travelcards can, for example, highlight the behaviour of millions of individuals and potentially allow associated digital CCTV images to be called up—without a person's knowledge or any effective governmental control. There is even the chance that this sort of data could be made available to third parties. Monitoring for congestion charging also has the potential—tied-in with ANPR (Automatic Number Plate Recognition)—if left unchecked to throw up similar problems.

7. Conclusion

Undoubtedly, CCTV plays an invaluable role with regards to crime detection and prevention in the UK and still maintains widespread public support—underlined by research undertaken by the Information Commissioner's Office (*Public Attitudes to the Deployment of Surveillance Techniques in Public Places*). It is therefore essential, moving forward, that checks and balances are adequately maintained—eg the Data Protection Act—to ensure that CCTV is not used inappropriately and that legislators closely monitor the potential impact of new technology on the privacy of individuals.

About Pauline Norstrom

Pauline Norstrom is a key figure in the development of CCTV standards. She is Group Head of Marketing at AD Group and Chairman of the CCTV Section of the British Security Industry Association (BSIA). Pauline also heads-up TC/10, a technical committee within the BSIA which looks at CCTV best practice and has been actively involved in the development of a standard for Digital Video Evidence and consultations regarding this issue on both sides of the Atlantic. Pauline is a regular speaker and writer on CCTV issues ranging from BS 8418 to the implications of Chip and PIN.

About AD Group

AD Group with its headquarters in Warrington, England, was established in 1997, its primary objective being to create and bring to market leading edge CCTV solutions. The pioneering nature of the Group's products, with the emphasis very much on R&D, has undoubtedly been a critical element in AD's success to date, receiving the Queen's Award for Enterprise: Innovation for its TransVu mobile CCTV system deployed on buses and trains.

19 June 2007

Memorandum by A A Adams, BSc, MSc, PhD, LLM, MBCS, CITP School of Systems Engineering

Summary

The move towards networked digital CCTV cameras, together with the increase in the related data featuring geo-location information (including electronic payment systems, mobile phone triangulation and GPS details and embedding of RFID chips) the role of the Surveillance Commissioners should be expanded and formal links with the work of the Information Commissioner established. In particular, following the *Durant v FSA* decision, there is an urgent need to clarify the status of stored data which does not link to an identified individual but for which an identification link would be relatively easy to establish, by both the legitimate holders of the data and by those who might gain access to the data by illicit means.

New *Surveillance Protection Principles* should be set forth in administrative guidance from the Surveillance Commissioners, and updated in line with technological developments, and should include the following with specific regard to CCTV:

- Clear announcement of CCTV recording.
- Photographs of operators (but not names and addresses) available to those surveilled.
- Licensing of operators and all others who have access to control rooms and raw data.
- Reasonable levels of security applied to transfer of images from cameras to control rooms.
- Where possible PETs to be implemented to prevent invasion of privacy.

In addition, the status of video data in criminal evidence should be made explicit:

- Clear rules of evidence to be applied to all systems suitable for use in possible proceedings.
- Disallowance as evidence data from any camera not subject to appropriate rules.
- Clear guidelines for police in requesting access to both live data and recorded data.

This submission is a shortened version of the attached appendix (not published), an academic paper published in the *Proceedings of EthiComp 2007*.

1. Introduction

Following the ruling of the Court of Appeal in *Durant v FSA* (*Durant v FSA* [2003] EWCA Civ 1746), raw video data is no longer regarded as Personal Data. This was never a suitable definition of such information, although the current definition that most video surveillance data is not protected is equally as bad. The current level of surveillance of UK citizens demands better regulation.

2. When is Raw Video Surveillance Data Personal Data?

In publicly accessible areas of the UK, video surveillance is usually lawful provided members of the public are notified that video surveillance is in operation. Provided that the organisation carrying out the surveillance is doing so within the law, the only protection for the surveilled is if the data is regarded as "Personal Data".

Despite the interpretation of the Data Protection Commissioner that raw video data constitutes "Personal Data", there are no well-known instances of Data Subjects making a request under the Data Protection Act 1998 for copies of all "Personal Data"held including raw video data. In some circumstance, such as victims of crime, those accused of crime and those involved in disputes with the police over possible malfeasance in the execution of police duties, individual citizens (including police officers) and law enforcement agencies have requested or required access to raw video footage.

The final judgement by the Court of Appeal in the *Durant v FSA* case changed the interpretation of the Data Protection Act 1998 radically. The Commissioner's current advice states [UK 05]:

> If you have a very basic CCTV system, its use may not be covered by the Data Protection Act.
>
> If your system is more advanced and allows you to zoom in on an individual member of staff whose behaviour is causing you concern, or you use cameras to monitor the movements and activities of your workforce, you'll need to inform us.
>
> If a general scene is recorded without an incident occurring, the pictures are not covered.

It would appear that it is the intent of the operator(s) of a surveillance system which defines the status of sections of data in the system. This does not provide a clear and useful boundary to the definition of status of data in recordings from surveillance systems.

3. Necessity and Proportionality Principles

In [Ba106], Graeme Gerrard of ACPO states that he wishes to see "proper regulation of CCTV to protect civil rights". However, he also would like to see both newly deployed systems and existing systems required to be "good enough for their recordings to be commandeered for use as police evidence" and "more compatible, that makes it easier for the police to access images". His interest in regulation seems more oriented towards making all CCTV systems useful and easily available to the police, rather than in protecting civil liberties. This pre-supposes that one of the primary purposes of CCTV should be to allow the police to access images.

In other discussions with UK police CCTV managers, it has been learned that future deployments of CCTV within, for example, the British Transport Police's areas will all comprise digital camera systems with network facilities to allow central access. In terms of value for money for a force as geographically spread as the BTP, which has responsibility for policing all of the UK's national rail infrastructure as well as the London Underground and (for some bureaucratic reason, various publicly owned underground car parks in London) this does indeed make sense. However, the broader the network infrastructure used to carry these images, the more vulnerable to external access this system becomes. Just as with the UK ID Card proposals and the NHS electronic patient records system, security of data on government networks seems to be something taken for granted without significant resources being spent on the security engineering.

Suggestions that privately deployed CCTV systems may be required to have a higher technological standard (which obviously opens them up to wider abuse of privacy than lower resolution systems) because they are therefore more use to the police in investigation and the CPS in prosecution, seems to be an unfunded mandate. In order to make any use of CCTV technology a company would then have to pay for it to be usable for police purposes. Whereas organisations such as banks, subject to the threat of armed robbery, might do well to heed the advice of police as to what standard of equipment and processing is needed to ensure utility

in criminal investigation, encouraging or mandating the update of existing or new systems over all would seem to be a recipe for increasing risk of privacy invasion without (once again) a significant study of the actual value this would produce in crime reduction or "clear-up".

The most worrying aspect of this is the suggestion that all new systems should be high quality, digital and networked. It is no large step to assume that the police would then press for "on- demand" access to both the live feeds and the recorded imagery for the purposes of manual and automatic tracking and analysis. However, much as the initial deployment of analogue CCTV in the UK happened with little public debate [NA99], the creation of a massive accessible network of high quality digital CCTV cameras in the UK would also present one of the biggest threats to individual privacy possible, when combined with the development of automated tracking, analysis and identification systems in projects such as REASON (www.reason-cctv.org), ISCAPS (www.iscaps.net) and AVITrack (www.cvg.rdg.ac.uk/projects/avitrack). The creation of such an infrastructure without clear explicit regulatory apparatus would be a grave mistake. Not only should the possible abuse by legitimate authority be considered, but also the worst case scenarios of the abuse of such systems by stalkers, crackers and general busybodies.

So, when considering both policy-level suggestions such as enforcing private CCTV systems to be higher risks to privacy, and in regulating licenses for the deployment of public and private systems, appropriate safeguards should be in place to consider the necessity and utility of the proposed systems and the potential costs not only in monetary terms to the public purse and the deployer, but in the risk to individual privacy that the system entails. Appropriate levels of security for high quality networked cameras should be required and their maintenance part of the ongoing licensing requirements. Appropriate logs of access should always be open to scrutiny by the appropriate regulatory authority.

4. Conclusion

Given the profusion of deployments of CCTV cameras in the UK and the profound threat to any form of anonymity of movement that expected further developments of CCTV infrastructure towards high resolution, colour, digital networked cameras represents, a law specifically defining the limits of valid CCTV deployment and use should be brought forward in the UK.

Given the nature of raw CCTV footage as not sensibly falling within the useful definition of Personal Data itself, and in the acknowledged utility of CCTV information for law enforcement purposes (although principally in after the fact investigation rather than live policing tasks, except in certain limited deployment scenarios), the principle regulator for CCTV should be the Office of the Surveillance Commissioners, whose role and resources should be expanded to provide licensing for public space CCTV schemes, guidelines on their deployment and operation and audit of the adherence to these guidelines. The OSC should, and already does where necessary, work with the Office of the Information Commissioner [OIC] to ensure that where video data is significantly processed to the point where it definitely becomes Personal Data, or where it is linked to other identification information such as payment or access controls, that both data protection principles and new Surveillance Protection Principles are being followed.

These Surveillance Protection Principles should include:

- Clear announcement of CCTV recording.
- Photographs of operators (but not names and addresses) available to those surveilled.
- Licensing of operators and all others who have access to control rooms and raw data.
- Reasonable levels of security applied to transfer of images from cameras to control rooms.
- Where possible PETs to be implemented to prevent invasion of privacy.

In addition, the status of video data in criminal evidence should be made explicit:

- Clear rules of evidence to be applied to all systems suitable for use in possible proceedings.
- Disallowing as evidence, data from any camera not subject to appropriate rules.
- Clear guidelines for police in requesting access to both live data and recorded data.

Acknowledgments

This work was supported by the EC (SEC4-PR-013800/ISCAPS) EPSRC (EP/C533402/1/REASON).

References

[Ba106] M Ballard. *Home Office to grab for more CCTV power.* www.theregister.co.uk/2006/11/22cctv_powers/ accessed 11.01.2007, November 2006.

[NA99] C Norris and G Armstrong. *The Maximum Surveillance Society: The Rise of CCTV.* Berg, Oxford, 1999.

[UK 05] UK Information Commissioner. *Obligations towards CCTV Systems.* www.ico.gov.uk/Home/for_organisations/topic_specific_guides/cctv.aspx accessed.

January 2007

Letter from Martin Beaumont, CCTV Manager, Cambridge City Council

1. Introduction

1.1 Although I hold the post of CCTV Manager for Cambridge City Council and lead the CCTV Users Group and Professional CCTV Managers Association on Training and Development, this evidence is submitted by me as an individual.

1.2 In this paper I would like to address the following issues:

a. Unregulated CCTV Cameras.

b. The Security Industry Authority Licensing Scheme for Public Space Surveillance CCTV systems.

c. The Information Commissioner and DATA Protection Act 1998.

d. The Human Rights Act 2000.

2. Unregulated CCTV Cameras

2.1 Prior to the release of this call for evidence, Lord Holme of Cheltenham, Chairman of the Constitution Committee is reported as saying "We now have close to 4.2 million CCTV cameras in the UK".

2.2 Where does this figure of 4.2 million come from? I do not believe that anyone actually knows how many CCTV cameras there are in this country and I am not confident that this figure is correct. However the real issue is that if we use the figure of 4.2 million then only about 500,000 to 750,000 cameras are subject to any sort of control.

2.3 These are the cameras used to monitor public spaces and are normally owned by local authorities. Although some private security organisations do operate some systems. Because these cameras are local authority owned, they are registered under the Data Protection Act and subject to the Human Rights Act, Freedom of Information Act, Regulation of Investigatory Powers Act and several Local Government and other pieces of legislation.

2.4 But what about the other 3.5 million CCTV cameras. These cameras are installed in commercial and private premises (people's homes), transport systems and other sites. Unless they register under the Data Protection Act they are completely unregulated and the owners can do what ever they like not only with the cameras but also the images they produce. I have had a large number of calls over the last few months from members of the public concerned that neighbours are invading their privacy but there is little we can do because there are no laws governing the private use of cameras. These CCTV systems must be brought under some form of control.

3. SIA Licensing

3.1 I was part of the committee, which assisted the SIA in establishing the Public Space Surveillance (PSS) CCTV Operators Licence. This was seen as an excellent system because for the first time minimum national standards of training and vetting were established before a licence could be issued.

3.2 Sadly the SIA's PSS CCTV Licence only applied to contractors. This immediately established a two tier system with those monitoring CCTV cameras for others requiring licences whilst those who looked after their own "in house" cameras did not. As a result, "in house" systems did not require licensing and so did not have to submit to minimum training or vetting standards. This situation is wrong and anyone who uses a CCTV camera to observe the public must be licensed.

4. The Information Commissioner and Data Protection Act 1998

4.1 The Information Commissioner has a massive responsibility and his office is always running to catch up with advancing technology. His Codes of Practice is already two years late. The approach they take should change and instead of trying to role all the technology into one, they should divide it up into smaller sections to enable them to keep abreast of the advances and changes in technology and working practices.

4.2 The weakness of the Data Protection Act is the reliance on people or organisations to register. If they do not register then there is little the Information Commissioner can do.

4.3 It is my belief that if the registration onto the Data Protection Act was dealt with in a similar way to TV Licensing ie when an organisation or individual purchases a camera, their details are passed onto the Information Commissioners Office so that registration under the Act can be processed. This would ensure we had an accurate figure of the number of cameras in the UK, what they are being used for and we could start to bring these 3.5 million CCTV cameras mentioned in paragraph 2.4 (above) under some form of control.

5. The Human Rights Act

5.1 My real comment on this Act is that we are missing a central point of information for Human Rights in this country. We need a Commissioner similar to the Surveillance Commissioner and Information Commissioner who can offer advice and guidance, update organisations on changes and legal cases, produce guidelines and codes of practices and conduct inspections and investigations.

6. Summary

6.1 There is plenty of legislation and regulation currently available to ensure that those organisations registered under the Data Protection Act or systems run by local authorities respect the rights of the citizens in this country.

6.2 However, the vast majority of CCTV cameras are unregulated, are not subject to any controls and drive a horse and cart through individual's rights to privacy. Whilst at the same time devalue all the hard work done by legitimate systems to obey the rules and respect the rights of the individual.

6 June 2007

Memorandum by Trevor Bedeman

Introduction

This evidence is in the form of a paper provided as part of a briefing on data sharing to an invited audience held at at Lovells law firm, London on 5 June 2007. The paper in no sense represents Lovells' views.

It addresses the current developments in both public and private data sharing, and is provided to the Constitution Committee for the comments contained on private development, comparisons between the two, and possibilities for their interchange. The comments just on the development of public sector data sharing are mostly drawn from the DCA Vision Statement and are thus not original.

There is, arguably, a great deal to be learnt from the private sector data sharing developments, some of which are either very mature, or very technically advanced, or both, and I would draw the committee's attention to the brief comments on private sector governance.

I am an independent consultant, specialising in data and information sharing. My past experience is as the lead author and negotiator of the "Principle of Reciprocity" which continue to govern the UK credit data scheme, and as previous Chairman of Insurance Database services Ltd, and Chair of the initial development of the Insurance Fraud Bureau. During this period I was an employee of LloydsTSB Group, latterly of the Risk and Compliance Department.

Data Sharing—Public Meets Private

Data sharing development in the retail private sector

Data sharing across the private sector has developed in more non-competitive areas of operational risk management, such as credit, insurance claims and financial fraud. Derivatives of that data support this processing, such as identity scores, and credit scores. Identity provides a common thread, and has been developed to a high level of sophistication.

Some of these schemes are very mature, for example the UK credit scheme dates from the late 1970s and shares 800 million records amongst 500 participating companies, with major economic impact upon retail credit and the larger economy. Some are highly advanced technically, for example in the derivation of identity, and the searching of the combined insurance claims and policy databases for networks of claims signifying organised fraud.

Within major retail groups such as those of the financial sector, the customer relationship management programmes of the 1990s on have meant that customer data is shared internally across many diverse constituent companies, and matched-merged into a single source for the entire group. Their ideal is that the entire individual customer relationship is available on demand at all customer touch-points and to the central analysis functions. These data sharing schemes can cover tens of millions of customers, and thus major fractions of the UK population.

Across competing private companies this commercial competition is an inhibition on the sharing of many forms of data. Companies are also under commercial pressure to handle this information safely. Individuals have some choice of processor through competition, and lapses of security are highly publicised.

The initial collector of the data has a key responsibility for the entire potential chain of use over the whole period that the data is held in any form.

This sharing is typically reciprocal, meaning that all available data within a defined sector must be provided before any other shared data can be accessed. The private sector has developed various models of sharer (and some wider stakeholder governance). The governance varies from the banking reciprocity committee SCOR, to trusts and companies such as the UK fraud avoidance scheme CIFAS, the Motor Insurer's Database, Insurance Database Services Limited, and the Insurance Fraud Bureau.

The next five years in the private sector

Credit data sharing is developing worldwide, with Experian as the first global scale reference agency, and there are various regional providers in development as well as nationally owned databases. The World Bank has assessed the UK's credit data sharing as the most effective, with the highest score of any scheme for the combination of availability of data (though not 100%) and efficacy of the regulatory framework.

Credit databases have developed in a similar way in the UK as in the US, though without access to a national identifier as in the US. There are some restrictive national databases in individual European countries, such as France, and other countries with models similar to the UK. It may be that the UK scheme will adopt the UK national identity when that is available; it will depend whether the quality of that identity is higher than that the banks already have through the current account and related financial products.

Individuals are increasingly searching their own data via the internet from the credit reference agencies. The uses are changing from those just driven by a failure to obtain credit, to a much more general need to regularly inspect the data held, for example as a protection against fraud. As in the US, it is likely that this shared data will come to be increasingly seen as also the property of the data subject, and not just of the contributing financial institutions, and thus the reference agency as also the individual's service provider.

Data sharing in and with the public sector

Cabinet committee MISC 31

This committee meets regularly at ministerial level to advance data sharing, with the aim of improving service efficiency. The terms of reference for this committee are: "To develop the Government's strategy on data sharing across the public sector".

The most complete statement of this strategy so far, and of public sector data sharing projects is contained in the document:

DCA Government Information Sharing Vision Statement

"This Government wants to deliver the best possible support to people in need. We can only do this with the right information about people's circumstances. We are determined that information sharing helps us better target support to the most disadvantaged in our society. The Social Exclusion Action Plan shows how Government will achieve this through agencies working together to focus on the unique needs of any one person or family. The information needed to make this happen already exists, but it is not always being shared.

That is why Government is committed to more information sharing between public sector organisations and service providers.

We recognise that the more we share information, the more important it is that people are confident that their personal data is kept safe and secure. This Government has an excellent track record of strengthening individual's rights to privacy and the legislative framework, provided by the Data Protection and Human Rights Acts, offer a robust statutory framework to maintain those rights whilst sharing information to deliver better services".

Catherine Ashton, DCA, September 2006

Existing examples of public sector data sharing

The Homelessness Act 2002 requires local authorities to review homelessness and share information. The Benefits have been assessed as including a 75% reduction in rough sleeping since 1998, and ending bed and breakfast accommodation for families with young children.

GMAC, Greater Manchester Against Crime, shares statistical information from a range of partners including health service, police, fire and transport, probation, and local authorities used to identify and map crime hotspots and determine how best to target resources across partner agencies. Example of benefits: 75% reduction in arson in some areas.

NFI, is the National Fraud Initiative run by the Audit Commission. It is a biennial data matching of housing benefit and employment records. 1,300 bodies took part in NFI 2004–05. The estimated value of fraud and overpayments in 2004–05 exceeded £111 million.

DVLA offers electronic re-licensing and off-road notification through internet and by telephone. The customer uses the renewal reminder sent by DVLA, or the reference number from the car's logbook and the vehicle registration number to identify the vehicle. DVLA links to MID, the Motor Insurance Database to check the vehicle is insured, and to the computerised MOT Test Certificate Database where necessary.

HMRC, DTI, DEFRA, FSA, and busness.gov are developing ITSW, the International Trade Single Window Project. The aim is that UK businesses will be able to provide information once, and ITSW will share this information with the main Government departments involved in authorising exports and imports. Initial phase estimated to save time for 150,000 small and medium-sized businesses and encourage others to trade internationally.

DWP uses HMRC income and capital information to contact those people who could potentially claim pension credit.

Future developments

The Social Exclusion Plan will provide for sharing across silos for the disadvantaged. Pilots will assess what information needs to be shared, such as police, housing and employment information.

In May 2006 the Police and Justice Bill was amended to allow information on the recently deceased to be shared more readily.

New Powers against Organised Crime and Financial Crime (Home Office July 2006) set out proposals for allowing public sector membership of CIFAS. The public savings have been estimated to be between £136–272 million per annum.

The Hampton Review recommended a principle be established that businesses do not need to give the same piece of information twice.

Sir David Varney's work on Service Transformation will consider the role of information sharing in improving the quality of service and result in efficiency savings for government.

DCA will be promoting better understanding of the DPA so that front line practitioners in particular understand that the DPA is not a barrier to appropriate information sharing.

DCA will explore how we might provide citizens with more information about which public sector bodies hold information and what they use it for.

The Serious Crime Bill 2007 has provisions in part 3 for the creation of Anti Fraud Organisations designated to share data on fraud between the public and private sector, such to and from CIFAS, a reciprocal fraudster reporting scheme, based traditionally in the retail financial sector.

Codes of practice

The Information Commissioner is developing guidelines against which information sharing proposals involving personal data might be assessed, and a framework Code of Practice which will help public sector organisations ensure that their sharing of personal information respects personal privacy.

Existing examples recommended as models include those of the Audit Commission 206 and NHS Confidentiality 2003.

Issues

"Sleepwalking into a Surveillance Society"

This phrase was originally coined by Richard Thomas August 2004 in response to the initial proposals for Government ID Cards. The "Surveillance Society" and the term "Privacy" have come to represent in part concerns over the wider sharing of personal data, especially by government, but also potentially by other parts of the public sector, and also within the private sector such as the risk schemes of credit and fraud. Both terms link visual records with symbolic data, and thus data sharing and visual surveillance are conflated. "Privacy International" recently ranked the UK along with a number of asian countries including China for very high levels of visual surveillance.

The Bulger case in February 1993 provided a public endorsement for CCTV cameras and so far for visual surveillance generally. In August 2002 the Data Protection Act had a close call with the Soham murders, when the act was initially claimed as a justification for not sharing information. The DCA Vision Statement advice to front line public sector practitioners shows that these issues are still live.

Street cameras are undergoing steady development, they can be miniaturised, and thus hidden; they may incorporate loudspeakers, as in a trial currently running in Middlesborough, and also sound receivers, to record conversations. Public acceptance of open air surveillance is not automatic, as speed cameras have shown, as has their vulnerability to a determined minority.

The private financial sector, too, has had a close call with public confidence, in this case over extreme debt. Concerns on over-indebtedness were led by press and Parliament; in this case extra data sharing has formed part of the solution, overriding commercial concerns over the sharing of valuable current account transactional throughput information by banks.

In both Houses of Parliament there are currently committees separately looking at issues of data sharing in the context of surveillance. The Commons Home Affairs committee is including a review of the extent and impact of credit data sharing. The Lords Constitution committee focuses on constitutional implications.

Time will tell what models data exchange between public and private will follow. It is likely there will be more examples of a data flow from private to public. The DVLA example brings many benefits to the individual in terms of time saved and efficiency of service, but no direct data flow in return to the contributing insurance companies, though all benefit from better vehicle licensing and the information flow can be inferred from the presence of a vehicle licence. The reciprocal data sharing scheme with associated governance has been the private sector answer to the balance of commercial advantage; the Serious Crime Bill provision for public sector data sharing with CIFAS is an example of the public sector joining in with an existing reciprocal scheme, and accepting its governance.

So far the public and private data sharing schemes are largely distinct, but as the public sector becomes far more interlinked, then it seems likely there will be greater interchange in addition between public and private, with implications not just for the commercial interest of affected companies, but of their staff and customers too.

References

Privacy and Data Sharing. The way forward for public services. Cabinet Office April 2002.
www.foi.gov.uk/sharing/index.htm

Public sector Data Sharing : guidance on the Law November 2003
www.foi.gov.uk/sharing/toolkit/lawguide.htm

Government Information Sharing Vision Statement September 2006
www.foi.gov.uk/sharing/

Code of Data Matching Practice 2006 (Audit Commission May 2006)
www.audit-commission.gov.uk/nfi/downloads/Code_Data_Matching_2006.pdf

Confidentiality: NHS Code of Practice (Department of Health 2003)
www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550

"Privacy International" National Privacy Ranking 2006— visual surveillance UK ranks 1 along with Phillipines, Singapore, Malaysia and China.

June 2007

Memorandum by the British Computer Society (BCS)

1. Scope

BCS has targeted both its Government Relations Group and its information security experts who have provided valued input in to this consultation.

2. Executive Summary

2.1 Whilst BCS supports the need for efficient public services which fully utilise the technology available, and understands the concerns which lead to the increase in surveillance measures, it is extremely perturbed about the increasing (although not deliberate) power of the state *vis-á-vis* the citizen as surveillance measures proliferate and data collection increases.

2.2 BCS wishes to warn policy makers of all the issues surrounding use of a "common identifier" in data sharing/aggregation and calls for adequate safeguards to protect the public in the light of this knowledge.

2.3 BCS believes the government should provide clear guidance on the guardianship of shared/aggregated data on individual citizens and recognize the importance of public trust and information assurance.

2.4 BCS believes that CIOs, SROs and Programme and Project Managers engaged in the Transformational Government Agenda should be professionally qualified to ensure that data is properly managed.

2.5 BCS believes that IT should be considered a Board issue and a major risk to the reputation and financial probity of an organisation.

Questions

1. *How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and state in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

1.1 Each individual leaves a detailed trail of personal information in public and private sector IT systems; on the Internet; and on CCTV systems. In the majority of cases, privacy is achieved through obscurity: for example, an individual may be recorded on a CCTV system, but in the absence of other personally identifiable information, their privacy is to all intents and purposes safe. Similarly, the presence of a few items of personally identifiable information in a computer system may not in itself comprise sensitive personal information about that individual.

1.2 However, Government[1] and industry are striving to improve the quality of the personal information that they hold. This usually involves consolidating the data into larger databases, and combining with other data about the individual. The government often refers to this as "data sharing" but the result is usually "data

[1] For example, the Transformational Government Initiative (November 2005) which involves using new technologies to create better services and efficiencies by moving towards a shared services culture.

aggregation", the joining of information together to form a larger, more detailed record (rather than indexing two separate records).

1.3 Data aggregation can be achieved either by using an existing unique identifier (such as a National Insurance Number) or by "fuzzy logic" to make probability decisions that two records do refer to the same individual. In either case, the record will be assigned a unique index number for future reference and ease of data recall.

1.4 The development of an identifier always creates privacy violations. Fuzzy logic invariably involves a "risk" decision, ie the system assigns a probability that given fields of data do refer to the same individual. Inevitably, there are errors where data is incorrectly matched and individuals find that inaccurate data about them is processed or published. The Credit Reference industry has gone to great lengths to resolve this.

1.5 Government is trying to introduce legislation that will create cross-departmental databases: at present there are approved and regulation "gateways" that prevent data being used for purposes other than that for which it was originally obtained. However, BCS is extremely concerned about data sharing/aggregation since the state risks losing public trust by continuing to share data without proper debate and safeguards. (Please refer to data sharing in the DVLA in the appendix).

1.6 BCS is agreed that the increasing use of surveillance techniques and the potential for data misuse demand rigorous processes and controls to ensure proper guardianship of the extensive range of information held by Government bodies and other organisations on individual citizens.

2. *What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might that line be identified?*

2.1 Surveillance and data collection should at all times be carried out within the Data Protection principles. BCS strongly believes in the need to guarantee that personal information will only be used for the purposes for which it was collected.

2.2 Data aggregation/sharing provides the potential to accurately retrieve data across numerous databases and build a picture of that individual's life that was not authorised in the original valid consent for data collection.

2.3 BCS believes strongly that there is a need to stimulate a public debate about the balance between efficiency and privacy in relation to information held about individuals. As a minimum, citizens should have the right to:

- free access to all the data that is held about them;
- correct errors;
- know who has access to it, and who has actually accessed the data; and
- challenge that access.

Most of this is intended by the DPA, but its provisions are in danger of being eroded.

2.4 BCS is also concerned about the need to secure data against malicious attack. Although this is covered by the Government's Information Assurance Strategy, the implementation of which is the responsibility of CIOs in all Government departments, in some departments this is seen as a "techy" concern and often delegated much too far down the organisation. BCS believes that IT should be considered a Board issue and a major risk to the reputation and financial probity of a department.

3. *What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

3.1 BCS believes that it is the unique identifier (described under Question 1) that presents the most significant threat to privacy and which is at the heart of an inadvertent strategy to build a surveillance state. Once an individual has been assigned a unique index number, it is possible to accurately retrieve data across numerous

databases and build a picture of that individual's life that was not authorised in the original valid consent for data collection. Often this is done with the best of intentions: for example, to identify children at risk by aggregating data from health, welfare, police and education sources. The consequence, however, is an unwarranted—and unauthorised—invasion of privacy of each individual within the system.

3.2 However, the greatest threat is the publication of that index number. Once it falls in to the wrong hands, it can be used to aggregate data across all the sources to which the perpetrator has access. The US Social Security Number is the most widely referenced identifier for each US citizen, and also the most widely abused.

3.3 It follows that BCS is concerned that the UK's current strategy of building a National Identification Registration Number—which will most likely be based on the National Insurance Number—will provide the catalyst for an escalation in surveillance and identity theft. The government has stated its intention of printing that number on the ID card which will be referenced in a host of government and commercial transactions. Positive outcomes will be an increase in public and private-sector efficiency, and a simplification of transactions for the data subject, but an unwanted side effect will be privacy violations. It is these that, if allowed to develop, will lead to the UK being described as a Surveillance State.

3.4 Quite clearly any form of surveillance will have an adverse effect on individual liberty. BCS believes that an acceptable balance must be struck between protection of society versus individual rights.

3.5 The Human Rights Act 1998 sets out provision for the "right to private life"[2] and it is this principle which will be affected by privacy violations.

4. *What impact do surveillance and data collection have on the character of citizenship in the 21st century, in terms of relations with the State?*

4.1 BCS members' views are polarised—some are happy with certain measures, eg CCTV cameras as there appear to be statistics that identify that they lead to reductions in crime. Others are very concerned, eg in the event of the improper disclosure of personal data leading to "identity theft." In such cases, one view is that there should be statutory compensation perhaps linked to the impact level in HMG IS1 to reflect the emotional and financial damage caused to the individual.

4.2 Other concerns raised by members include: the storage and retention of fingerprints and DNA data of innocent people on databases; the covert use of telecommunications traffic data for tracking mobile phone and recording internet usage.

5. *To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?*

5.1 BCS believes that the provisions of the DPA are more than adequate but is concerned that its provisions are still not being properly adhered to, particularly in the private sector, despite being 1984 legislation, updated in 1998. The public sector (particularly at Local Government level) is mature in its implementations of information governance compliance. However, legal advice in different departments, agencies and organisations varies with respect to the interpretation of the DPA in specific circumstances. In particular, interpretations are being tested in the courts in relation to the provisions of the Human Rights Act.

5.2 BCS respectfully suggests that care should be taken when producing legislation to ensure that it does not appear to conflict with the DPA. For example, the Government, through Connecting for Health (CfH), is apparently offering an "opt-out" to patients with respect to their personal data on the central spine system. By doing so, the DoH (through CfH) is assuming that it is a data controller under the Data Protection Act, whereas most patients think their medical professional is in control. This claim to be a data controller arises since the obligation to offer the right to object to the processing[3] falls on a data controller. It follows that the DoH—and the Secretary of State—by offering an opt-out considers it is a data controller (eg with respect to the NHS spine).

5.3 This complexity and lack of legal clarity hinders the Government in its determination to deliver a transformed public service based on active (and yet secure) information sharing.

[2] Article 8—The right to respect for private and family life, home and correspondence.
[3] Section 10 of the Data Protection Act 1998.

6. *Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

6.1 The solution is not to regulate the collection or processing of data—the Data Protection Act (1998) is already adequate for this—but instead to control the assignment, use and dissemination of common identifiers about the individual. Where the state assigns a "trusted" identifier to an individual, this should not be published, shared with the private sector, or relied upon as a sole identifier in the absence of other identifying information (such as a name, address, signature etc). Where the private sector applies such identifiers, the Information Commissioner's Office should be given greater support to enforce the correct and valid processing of this sensitive personal information. Prudent and practical legislation is now essential if we are to provide constitutional protection for privacy for future generations.

6.2 The majority of the UK citizens have a mobile phone that is a tracking device in its own right since it is permanently emitting a GPS signal. The communication traffic is also stored in a several locations. The European Data Retention Directive is seeking to implement a legal requirement to retain the traffic data (not the content) for a specific period of time in case it is required to assist in the investigation of a crime. BCS believes that the existence of the information does not warrant its utilisation for anything other than a specific purpose for which a Privacy Impact Assessment has been undertaken.

6.3 In addition, because of the new government emphasis on "a presumption of sharing" and notwithstanding guidance from the DCA, the original collector and owner of personal data should have a duty of care with respect to that data to ensure any organisation sharing it understands any caveat associated with its integrity and appropriateness for use for purposes other than that for which it was originally collected (eg has it been verified or is it interpretation and hearsay, when was it collected and does it have a finite useful life, has it been cleansed).

6.4 This is particularly important in relation to such things as the proposed summary care record. At present the patient record is held and maintained by the citizen's GP. Once it moves to the spine, it will be possible for other (eg hospital or walk-in-centre clinicians) to add to it. GPs are reluctant to retain responsibility for data added or amended without their having seen the patient and it is unclear who would have guardianship of the integrity and accuracy of the central record.

7. *Concluding Remarks*

7.1 BCS recognises that no democratic government seeks to undermine civil liberties deliberately through the construction of a surveillance state. However, it is evident that such an outcome arises not due to the deliberate intention of the state, or any private sector body, but rather the failure to prevent the sharing and aggregation of data without suitable privacy safeguards.

7.2 The issues raised in this paper have been debated by participants at a thought leadership debate, sponsored by BCS Government Relations Group (GRG), in October 2006, with further material from BCS's IPEP[4] in particular. BCS is working in this area and would be very happy to provide further advice to the committee as and when it feels it to be appropriate.

6 June 2007

APPENDIX

DATA SHARING EXAMPLE—DVLA

What data does DVLA hold on citizens and who does it share that data with?

The DVLA registers hold data included on a driving licence application or renewal, vehicle keepership and on vehicle road tax payments and renewals. The personal data includes: name, date of birth, address, phone number (voluntary), photo, signature, gender, vehicle types individuals are entitled to drive (and record history of each), points on licence, whether disqualified or not.

So the DVLA holds information on people's identities, notified contact address, vehicles they hold as registered keepers and financial data in respect of their payment of Vehicle Excise Duty. The vehicle keeper data are also available to anyone who has reasonable cause eg wheel clamping companies and insurance companies. This is a statutory requirement and the vehicle keeper is not therefore consulted about access.

[4] The BCS Information Privacy Expert Panel (IPEP) The BCS Information Privacy Expert Panel is responsible for establishing and maintaining the position of the BCS as an independent voice of authority within the field of information privacy.

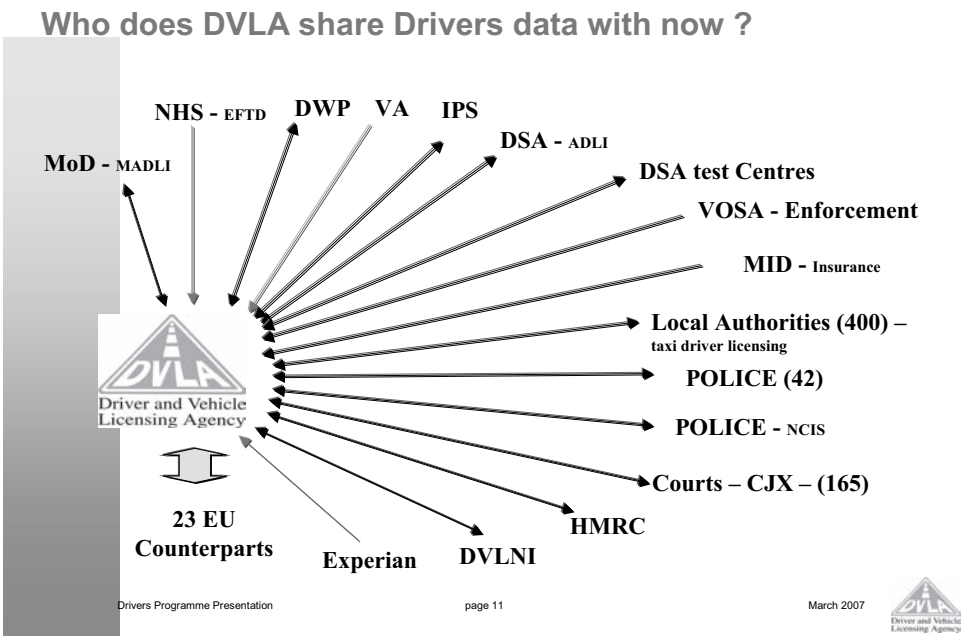
Currently, the vehicle systems have no functionality that allow this to be logged in an audit trail that can allow keeper review.

Few citizens would be concerned about the degree of data sharing by DVLA (see the diagram below). However, a series of Government initiatives and law changes could potentially result in sharing this data more widely. DVLA is more likely to become the recipient of data from a wider range of agencies, particularly in respect of authentication of identity (result: fewer fraudulent records) or address change notification (result: citizens would have to notify fewer agencies). These changes include:

— MISC31—DCA review of barriers to data sharing—report May 2007.
— Review of Information on Criminality—Home Office—January 2007.
— Serious Crime Bill.
— Criminal Justice Bill—May 2007.
— ID Card Bill—2006.

There is pressure to harmonize this access for motorists and vehicles across the EU. Countries across the EU have very different cultural and legal frameworks, in which interpretations of the basic (European-wide) Data Protection legislation vary. This makes the sharing of data complex. The call for this sharing is as much public (eg foreign vehicles parking in London, avoiding speeding fines) as it is governmental (road safety, crime reduction).

Who does DVLA share Drivers data with now?



Memorandum by the British Security Industry Association (BSIA)

The British Security Industry Association (BSIA) is the trade association covering all aspects of the professional security industry in the UK. Its 570+ members provide over 70% of UK security products and services and adhere to strict quality standards. The BSIA represents the manufacturers and installers of CCTV systems and those that run Remote Video Response Centres.

SUMMARY

CCTV is a vital weapon in the prevention and detection of crime and in reducing fear of crime. It is used comprehensively as a tool by the Police and contributes significantly to the evidence produced in thousands of investigations obtained from publicly and privately operated systems. The use of CCTV has changed the individual's relationship with the state, increasing the sense of security of the individual. Privacy is protected both through current legislation, industry guidelines and codes of practice, and by continued legislative consultation as CCTV technologies become more sophisticated. As technology develops with the move from

analogue to digital recording and, more recently, the introduction of more sophisticated event detection techniques through video analytics capabilities—new uses of CCTV become common practice. Therefore, it may be necessary to review common legislation and standards in order to continue to protect the privacy of the public.

Increased use of CCTV

The application of CCTV has increased significantly in the past thirty years thanks to the successful use of the technology by businesses, the public sector and the Police in the prevention and detection of crime and today the UK is acknowledged as the world leader in this field. This has inevitably changed the individual's relationship with the state as individuals are now subject to surveillance when they are in public spaces, travelling on trains and buses and within some business environments. However, a crucial point to make is that the privacy of individuals is protected on a number of levels thanks both to legislation and to the self-regulation of the industry through compliance with British Standards and other codes of practice.

In this uncertain world, other countries are following Britain's example by expanding their CCTV infrastructure. For the French, events such as 7/7 in London—and the acknowledged value of CCTV evidence—have made them think again about CCTV restrictions and where the balance between security and personal freedom lies. A bill introduced at the end of 2005 opened up the use of CCTV in public areas, including the transport network.

Protective Legislation and Standards

A number of pieces of protective legislation have been introduced to safeguard the privacy of individuals. The Data Protection and Human Rights Acts both protect people from misuse of CCTV. We believe that the Data Protection Act is a robust piece of legislation, but must be actively implemented, offences investigated and offenders prosecuted.

CCTV operatives that monitor cameras in public spaces now have to hold a Security Industry Authority licence and must be subject to a criminal record check and comprehensive training. The security industry imposes its own standards through membership of the British Security Industry Association and independent inspection by a UKAS accredited certification body. The BSIA proactively works on guidelines to protect personal information. For example, the Association recently produced a Privacy Masking Guide which provides guidance on how to restrict what can be seen by CCTV. Thus, privacy is safeguarded through the application of best practice.

The Balance Between Privacy and Security

There has to be balance between individual privacy and the duty of the state to provide effective security measures for the benefit of all. Surveillance is a means by which the state can provide security, as it can prevent and detect both serious and minor offences. It also plays a significant role in reducing fear of crime.

In a private place an individual can reasonably expect not to be under the state's or other surveillance, which can only to be departed from under strict regulation. In public, individuals may be observed by CCTV, but should expect this to be carried out under strict guidelines.

CCTV in public places does not curtail or prevent individuals doing anything that they could not in any event lawfully do. It observes, in most cases unobtrusively. CCTV is on occasion used for unlawful means, such as capturing the PIN number of a customer using a credit card, but these are examples of old offences being committed in new ways. The key to ensuring that CCTV is not abused is covered by rigorous rules as to how CCTV data is stored so that access cannot be given to unauthorised personnel. It is also imperative that CCTV cameras are positioned so that their view does not impose on private premises. Hence, the BSIA has developed guidelines on CCTV and Chip and PIN and Privacy Masking which can be downloaded at www.bsia.co.uk/publications.

Research which speaks to people on the ground such as that undertaken on behalf of the Information Commissioner's Office—"Public Attitudes to the Deployment of Surveillance Techniques in Public Places" tends to reflect a recognition of the benefits of CCTV. In this case those interviewed tended to "feel safer where CCTV is installed", seeing it as "an anti-crime measure both to deter criminal and anti-social behaviour, and to catch the perpetrators."

The use of CCTV by the Police

Many offences are currently only detected by the Police through the use of CCTV. It is now an essential tool in the investigation and detection of crime.

CCTV played a significant part in identifying the London bombers on 7 July 2005 and the attempted bombings two weeks later. These events have certainly underlined the vast improvement in the quality of CCTV evidence available to the Police compared to that provided in past incidents. For example, in the Jamie Bulger case 14 years ago the limitations of the low contrast images collected are frequently referred to as an example of poor CCTV, not withstanding the tremendous assistance that this evidence provided to the police in locating the murderers. By contrast the quality of evidence captured on buses, trains and stations in London has been noted by the public and press alike as being of high quality and has proved invaluable to the authorities in apprehending the suspects connected with the failed attacks on 21/7. Much of this change can be attributed to the advent of digital recording, improved camera technology and the extensive nature of the CCTV infrastructure we now have in the UK.

Impact of New Technologies

New advances in CCTV and similar technology can screen for particular patterns of behaviour through the use of video analytics. This has the potential to identify serious crime, terrorism and more widespread, less serious offences. Facial recognition is also likely to emerge as a technology which could assist with border controls, air travel etc. At the moment, it is a fledgling technology, but more research and investment could reap real rewards. The National Police Improvement Agency is looking at how facial recognition technology can be used with the police facial images database to potentially allow automated recognition of 'wanted' police suspects.

There is growing interest in remotely monitored, detector activated CCTV—complying with the BS8418 Code of Practice—which has demonstrated its ability to stop crime on commercial and public sector sites across the UK and, crucially, to assist the police to apprehend criminals. The overriding attraction of this form of CCTV is the fact that there is visual confirmation by an operator regarding the cause of a specific activation.

Continued Legislative Consultation

As new technology develops and becomes more widely used, consideration must be given as to whether our current legislative and standards controls are robust enough to cover such use. The BSIA regularly puts together guidance and codes of practice on such issues and will continue to do so.

There is a fine balance between public safety and the individual's right for privacy. This balance will change as CCTV technology becomes more sophisticated and the individual's identity is able to be captured automatically. Continuous monitoring of CCTV technology by the Information Commissioner, with support from other departments such as the Home Office, would ensure that any changes in legislation in order to maintain the balance between the individuals' privacy needs and the state's requirement to protect the public could be enacted by Parliament.

Conclusion

CCTV is now an established tool used by the Police, with a proven record of preventing and detecting crime and reducing fear of crime. Its use in public places is already regulated and should continue to be so. As technology develops and new uses of CCTV become common practice, it may be necessary to review common legislation and standards in order to protect the privacy of the public.

8 June 2007

Memorandum by The Customer's Voice

1. This response to the your consultation exercise is on behalf of The Customer's Voice (www.the-customers-voice.com), one of a new breed of person-centric service provider focused on providing professional-grade information management services to individuals.

2. Before responding to the specific queries raised in the consultation, it is worth introducing our perspective in more detail. This is best achieved through reference to the quote below from the National Consumer Council:

3. The quote below from the National Consumer Council in 2004* neatly summarises the dilemma being addressed in this consultation exercise.

> "Personal information is one of the most valuable commodities in society today. Government and public service providers gather a wealth of information from taxpayers, car owners, benefit recipients, patients, clients, customers and voters. Businesses too, are intent on developing ever more sophisticated ways of capturing and using data about individuals.
> Consumers have much to gain from these developments. But whenever personal data is collected and stored it may also be abused. Wrong information may be passed on to third parties, privacy invaded, or individuals besieged by marketers. Trust is hard won and necessarily fragile. If the information age is to develop on secure foundations, it is vital that those who collect and use personal data maintain the confidence of those who are asked to provide it."
>
> *The Glass Consumer, 2004
>
> *Source:* National Consumer Council, 2004

4. This statement rightly draws attention to the fact that individuals can gain much from the developing information age. But, the reality is that individuals have an ever-growing body of evidence that suggests they should be very wary of what they provide and who they provide it to when they are asked to share personal information. In recent years individuals have been increasingly exposed to:

5. The rapid increase in the use of surveillance and tracking technologies with little in the way of "opt out" possibilities.

6. An ever-growing mountain of irrelevant junk mail on their doormats, and other forms of direct marketing messaging grabbing their precious time.

7. Cold-call tele-marketers blatantly using hard sell "slamming" tactics to sell products and services that are not in the individuals' best interests.

8. Their personal data being sold, bought, rented and swapped for money, in which they get no share (even public sector bodies such as the DVLA have managed to justify to themselves and their pay-masters that selling personal data is within their remit).

9. Inaccuracies in personal data stored by the information industry that take individuals significant amounts of time and effort to correct; if, of course they even find out about them.

10. The increased risk of identity theft, with all that this entails, from organisations taking less care of personal data than they should.

11. The team involved in The Customer's Voice proposition has many years combined experience of customer management and customer information management within large organisations. Our decision to focus on providing information management services to individuals is, in many ways, an indictment on current organisational approaches. There are solid structural reasons why organizations in both private and public sectors wish to do more with personal information than the subject would ideally have them do. Private sector have the profit motive and their shareholders demand that they extract maximum value—hence the behind the scenes sale of customer records. The public sector also has obligations to stakeholders—most often round cost reduction and national security—they will always act accordingly and deliberately do more with personal information than the subject would wish.

12. The only route through this scenario is the acceptance that over time the individual (or more accurately their agents) will become the dominant provider of information to the organisations that serve them. This will come about through technology (eg digital identity), legislative and commercial change—the latter dominating, the former being an enabler.

13. Specific responses to the questions raised in the consultation exercise are shown below.

Questions

1. *How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and state in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

15. Little change of any real consequence has as yet taken place—largely because of the inadequacies of recent deployment. Luckily, we live in a society that is more than capable of shining a light on radical proposals or activities and at least having them watered down to the point of being relatively benign.

2. *What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might that line be identified?*

16. Un-controlled personal data sharing across government and then allowing the big banks and the credit bureaux to tap into this is the point at which things become dangerous.

3. *What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

17. Human rights are regularly breached, as are Data Protection and Electronic Privacy rights—but none are articulated at the level that would allow these breaches to be meaningfully tackled.

4. *What impact do surveillance and data collection have on the character of citizenship in the 21st century, in terms of relations with the State?*

18. Trust in government is falling and will continue to do so, with surveillance and data related issues one of many reasons for this. Ultimately this impacts on democracy as ever increasing numbers don't bother to vote or participate.

5. *To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?*

19. The Data Protection Act is now weak in a number of areas:

— Generically, it is articulated at far too high a level to be meaningful, personal data types (we list 75 types in our work) must be listed and described in detail, as must personal data uses (we list 90 types seen within organisations).

— Mandatory and immediate notification of data breaches should be included, with compensation and paid for fraud protection built in.

— The principle of Subject Access should be extended to allow the subject to request constant access to personal data being stored (via a data mart within the data processor), and regular electronic copies of the data should be sent on request in a standard (XML based) format.

— "Opt In" should be the default position across all forms of marketing communication.

6. *Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

20. Yes, there is undoubtedly a need for a significant upgrade in constitutional rights around personal data. This can best be achieved through taking a radically new perspective and then updating current processes accordingly. That new perspective must be based on a recognition that over time, the enabled and empowered individual is the best (most current, most accurate, most relevant) source of the data inputs for many processes across government and private sectors. This subject is expanded upon further in a white paper available at http://www.rightsideup.net/documents/PersonalKnowledgeBanksrevise2_000.pdf.

This change is inevitable and already underway; the technology is almost in place through which individuals can assert their own identity claims (open ID). The role of government in this space is to enable it. This can be done by acting as an identity service provider to the citizen/resident base, and by leading the way in terms of providing data access in electronic forms.

7 June 2007

Memorandum by the e-Assessment in Child Welfare research project, located at the University of Huddersfield and part of the Economic and Social Research Council e-Society Programme

Dr Christopher Hall and Dr Sue Peckover (Huddersfield University), Professor Andy Bilson (University of Central Lancashire), Professor Brid Featherstone (Bradford University) and Professor Sue White (Lancaster University)

Summary

This submission reports findings of research on the implementation of new technologies to support information sharing and assessment in child welfare—the children's database and the common assessment framework. There has been concern that the database constitutes an increase in surveillance of families and an invasion of privacy. Our findings are that the implementation of the technologies has been slow with some reluctance by professionals and agencies. There are problems about accuracy, consistency and consent. The use of new technology also provided challenges to working in partnership with families. The extension of the initiative with the implementation of a national database, ContactPoint, poses major concerns about privacy and constitutional rights.

1. This submission reports the findings of research by the e-Assessment in Child Welfare project, located at Huddersfield University, part of the ESRC e-Society programme. The project has monitored the implementation of the Information Sharing and Assessment initiative in four local authorities over the last two years, including two of the pilot projects. Our findings focus on how these technologies are being used by professionals in their everyday work.

2. Information Sharing and Assessment

The Inquiry into the death of Victoria Climbié, (the Laming report), like many that preceded it, highlighted problems in the way that professionals in child welfare communicated. They often worked in isolation, had a partial view of the needs of and risks to Victoria and made unwarranted assumptions about the role and actions of other professionals. Had information available to these professionals been coordinated, a more holistic picture of Victoria might have emerged and the need to intervene been recognised. In response the Government introduced the Children Act 2004 and the "Every Child Matters" initiative, which implements new technologies to promote information sharing and assessment of children: the children's database (sometimes called the Child Index) and the Common Assessment Framework.

3. The database has been the subject of critical comment in Parliament, the media, amongst children's charities and academics. Some consider it an inappropriate, costly and disproportionate response which will not protect children. Too much information will be collected but without extra services. Others see it as an invasion of family privacy and an increase in surveillance more generally. There are particular concerns about the security of confidential information.

4. The Children's Database

The children's database is required under s.12 of the Children Act 2004. It contains basic information on all children in an area, details of their parents and carers, school and GP. It also includes contact details of targeted services being provided and the opportunity for professionals to record a "cause for concern". It is accessible to all professionals with criminal records bureau clearance. It does not include confidential information or case records, but indicates where such information exists. However it has been noted that displaying children's contact with services and "concerns" constitutes confidential information. It was piloted in 11 local authorities, but, because of technical and information sharing problems, only three have established a working index. A national database (called ContactPoint) is planned for 2008.

5. The Common Assessment Framework (CAF)

The CAF has received less comment. This is a standard assessment form to be used by all child welfare professionals, which can be e-enabled. It encourages professionals to assess children in terms of their personal development, parenting and family environment, under 19 headings. Children and parents' comments and their consent to share the assessment are recorded. The existence of a CAF is entered on the children's

database. It is seen as an early assessment of a child's needs and concerns, to be completed mainly by schools, GPs, health and early years' professionals. The CAF was piloted in 12 local authorities and is being developed in others.

6. Context of ISA

The development of these technologies should be understood in terms of changes in child welfare policy more generally. Social policy commentators have observed the expansion of state intervention with children. "Every Child Matters" heralds a more universal view, focusing on "children with additional needs", rather than children "at risk" or "in need", as in earlier legislation. The Government aims to identify and track around a third of children who require interventions beyond universal services. By intervening at an earlier stage, it is hoped that more appropriate services can be provided and more serious problems prevented. However, such identification requires a massive system of assessment and information exchange. The use of information and communication technologies (ICTs) can be seen as constituting increased surveillance of children and families. In particular, information at early stages of "concern" is being recorded and shared, some of which might be termed "low level"; for example children with literacy difficulties who did not warrant a holistic assessment. In our research some professionals were instructed to complete CAFs routinely, sometimes with insufficient knowledge of the child. The database includes all children, yet only a small proportion have needs which warrant multi-professional attention. This raises the question whether these are proportionate responses.

7. Whilst child welfare organisations have always maintained large amounts of information on children, these initiatives encourage and require information to be managed and exchanged in new ways. The ICTs in the pilot projects in our research have limited functionality, only able to track individual children. However, it is not clear what options will be built into ContactPoint, and if it will facilitate opportunities for "data matching and profiling" (combining data sets to predict behaviour) or "function creep" (data collected for one purpose are used for another).

8. Inaccuracies

Our research has identified wide data inaccuracies. In terms of the children's database, there are both technical and practice problems. A child's record was established by matching data from various sources, health, social services, education and because of differences in basic information—names, house numbers, birth dates etc—this created multiple records for some children and missed others. Children who frequently change address or school are often particularly vulnerable.

9. There was inconsistency over when a professional should indicate their involvement with a child on the database. For those in contact with large numbers of children, for example teachers or GPs, it is not clear at what point their involvement constitutes more than a universal service. The pilots demonstrated that when parents were consulted before making an entry, some refuse. Also some "sensitive services", like counselling or mental health workers, did not record their involvement. All these omissions and errors meant that a professional looking up a child's record did not see all those involved. In our research, the local knowledge of workers was often more accurate than the database. This created a view that the database was not useful and led to less use and hence more inaccuracy.

10. Inconsistent Practices

We found considerable variation in the use of the CAF, both between and within local authorities. Some agencies see it as an internal assessment for the professional, the family and the agency. Others see it as a referral to pass concerns on to targeted services. Different uses create different approaches to how it is completed. The former approach is more likely to be completed with the family and represents agreement about a shared view of the child. The latter aims to persuade other agencies to become involved, not necessarily representing families' points of view.

11. Information sharing is often assumed to be straightforward: for the writer it is seen as uncontested, discrete and easily written. For the reader it is seen as accurate, consistent and meaning the same thing. However we found professionals balancing dilemmas of working in partnership with children and parents and sharing concerns with other agencies. In both cases information sharing was a strategic activity.

12. Consent and Partnership

Obtaining informed consent to share CAF information is difficult with electronic systems. Our research found no evidence children or parents had access to their electronic records, and consent to record professional involvement was not clear. Some professionals completed CAFs with children and parents, but, particularly when used for referral purposes, only around half reported consent. As these technologies are extended, they limit the active participation of children and parents in key decisions across increasing parts of service provision.

13. The database and CAF concern individual children and there is limited ability to address wider issues in terms of families and communities. The limited functionality of the database does not link siblings' records. The CAF asks about parenting, not the problems faced by parents. To assume that CAF databases have more accurate information about services than families may encourage a general distrust of parents.

14. The Future Implementation of ContactPoint

A number of constitutional issues are raised by current proposals for ContactPoint. This includes removing the need for consent and common law rights to confidentiality with regard to data held on it. We are also aware of the draft guidance on shielding (hiding) data in ContactPoint which makes it difficult for individuals (eg those involved in domestic violence) to know of the need or to request that their data should be shielded. The proposed threshold is that data can be withheld only if it is likely to cause "significant harm". With potentially a wide range of professionals accessing ContactPoint there are insufficient safeguards. Whilst the data are limited, malevolent access raises serious potential misuses (eg grooming a child, locating estranged children or stalking a professional).

15. Given this impact on constitutional rights and potential misuses, ContactPoint needs to demonstrate that it serves the greater good either through demonstrating general benefits to a wide range of children or substantial benefits to a smaller number. As with other commentators we question whether the specific benefits of the system are likely to be achieved sufficiently to outweigh possible problems of confidentiality, inaccuracy or potential abuses of the system.

6 June 2007

Memorandum by Charles Farrier

This submission has been prepared specifically for the Committee. I am submitting this as an individual. I am an IT professional with 15 years experience working in software and website development. I work extensively with databases and am aware of the dangers inherent in them.

Executive Summary

1. The unchecked growth of the surveillance state in the UK threatens our way of life and many of our most basic freedoms are at risk. Each new measure that is introduced may appear harmless when looked at in isolation but when pieced together they create powerful instruments of social control that pave the way for an authoritarian state. There is much talk of "joined up government" but little joined up thinking it seems when it comes to the society that is being shaped.

2. Safeguards need to be put in place to protect UK citizens, bills before parliament should be subject to rigorous privacy impact assessments. It is not acceptable for the state to remove long established freedoms under the cover of a perceived threat that will "last a generation".[5] All legislation that surrenders freedoms should have sunset clauses.

3. The introduction of identity cards and the powerful database behind them has profound constitutional significance and so it will be the main focus of my evidence, though many of the issues are true for other surveillance enabling technologies and legislation.

Identity Cards

4. The constitutional significance of the Identity Cards Act, as the committee has previously pointed out, is that: "it adjusts the fundamental relationship between the individual and the State".[6] At present the state is answerable to the citizen, the citizen is not answerable to the state for his identity. Citizens use purpose specific identifying materials rather than a single compulsory identifier. This affords the citizen some degree of privacy and control over the data that is held and how it is shared.

[5] *Blair warns of 'long struggle' with terror*—http://news.independent.co.uk/uk/crime/article1963150.ece
[6] House of Lords Select Committee on the Constitution, 5th Report of Session 2004-05, HL Paper 82.

5. No comparable system of the size or level of intrusion proposed by the Government has been introduced anywhere in the world. Meanwhile other nations have stronger checks and balances in place. For instance: France and Germany have no national identity register, Germany has a very strong privacy law and has constitutional limitations on the establishment of any national identity number.

6. The level of surveillance that the Identity Cards Act enables is a threat to a many of our most basic rights; including our right to privacy, freedom of movement, presumption of innocence, freedom from arbitrary arrest and confidentiality of personal records. Identity cards and their associated database go against our common law tradition of liberty and respect of the rights of the individual. What is more they undermine the principle of trust.

7. In the absence of a written constitution, the identity card scheme could be extended by a simple majority in the Houses of Parliament. Currently there is something of a constitutional crisis, whereby the House of Commons has supreme legislative power thanks to the Parliament Acts of 1911 and 1949, allowing a bill to be passed even if the House of Lords reject it. This situation was described by Lord Hailsham as "an elective dictatorship", whereby "the Government controls Parliament, and not Parliament the Government".[7] Lord Scarman, the first chairman of the Law Commission warned that: "When times are normal and fear is not stalking the land, English law sturdily protects the freedom of the individual and respects human personality. But when times are abnormally alive with fear and prejudice the common law is at a disadvantage: it cannot resist the will, however frightened and prejudiced it may be, of Parliament."[8]

8. The Government's scheme is not just a piece of plastic with your photo on it. A powerful infrastructure will be created with a giant centralised database at the heart of it. This database will facilitate a hitherto unknown level of day to day surveillance of UK citizens via (1) data sharing (facilitated by the unique National Identity Register Number) and (2) dataveillance[9] (via the database's audit trail).

9. The United Kingdom has no clearly defined privacy law, so it is unclear whether sufficient checks and balances are in place to protect privacy. Both the Information Commissioner and the Law society called on the Government to undertake a Privacy Impact Assessment before progressing with the bill but there calls went unheeded. All bills before Parliament should be subject to such a privacy assessment.

10. Because of it's reliance on technology and databases the government's scheme runs the risk of binding future government's, as it will not be easy to undo once it has been put in place.

11. During the passage of the Identity Cards Bill through Parliament the Joint Committee on Human Rights raised 14 points of concern with regards to the bill.[10] In his response the Home Secretary said: "I consider that all the powers in the bill are capable of being exercised compatibly and its human rights compliance has to be judged ultimately by looking at the bill and all the orders and regulations made under it."[11] A fundamental principle of our constitution is the rule of law. Mr Clarke like all too many ministers today appeared to be proceeding under the rule of person.

12. Without the proper checks and balances in place, such as a privacy law, the power of courts to strike down unconstitutional legislation and an effective second chamber, the passing of the Identity Cards Act is a worrying and dangerous development. It has handed the tools of totalitarianism to an elective dictatorship within a climate of fear.

Conclusions

13. The constant and unquestioning use of modern surveillance technology in pursuit of a risk free world is folly. There is already a shift from detecting crime to predicting crime before it happens. It is not difficult to imagine a future where surveillance systems that could know what every citizen is doing at any moment in time. Such systems could be used to try and pre-empt crime using computer based profiling techniques but at what cost? If left unchecked society will become imprisoned rather than liberated by technology.

14. Concepts such as "implicit consent" are being used to hide the fact that citizens increasingly have no choice in the way in which they interact with the state.

15. There is an urgent need for clear unbreachable boundaries to be created to protect the citizen from unnecessary intrusions of the state. Currently all too easily citizens' privacy and freedom are compromised in the interests of national security, to fight crime or to facilitate the smooth running of public services.[12]

[7] The Richard Dimbleby Lecture 1976.
[8] Hamlyn Lectures, English Law—The New Dimension, 1974.
[9] See *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV
[10] Joint Committee on Human Rights, Identity Cards Bill, Fifth Report of Session 2004–05 (HL Paper 35, HC 283).
[11] http://www.homeoffice.gov.uk/docs4/HS_Reply_Joint_Committee_Human_Rights.pdf
[12] See Section 1(4) of the Identity Cards Act 2006.

16. "As a society, we want to say: Here you may not go. Here you may not trade and analyse information and build dossiers. There are risks in social anonymity, but the risks of omniscient and omnipotent state and corporate power are far worse."[13]

7 June 2007

Memorandum by the Finance & Leasing Association (FLA)

Introduction

1. The Finance & Leasing Association (FLA) represents the asset, consumer and motor finance industries. Our members provide secured and unsecured personal loans, credit and store cards, leasing, hire purchase and asset finance of all kinds. New business in 2006 amounted to £93 billion, including £66 billion for consumers and £27 billion for businesses and public services. 30% of all the investment in fixed assets (except real estate) in the UK in 2006 was provided by FLA members.

2. This contribution to the economic well-being of individuals, businesses and public services is only possible if our members are in a position to take responsible lending decisions. This means having the relevant information on which to base such decisions. Without such information, there is a high risk of fraud and money-laundering, and of customers becoming over-indebted. We are therefore strong advocates of responsible data-sharing, and of the robust controls which already exist to ensure that access is restricted to those who have a legitimate need for such data.

3. The FLA welcomes the opportunity to participate in the Lords' Constitution Committee's inquiry. The rest of this submission deals with those topics listed in the call for evidence on which we feel qualified to express an opinion.

Our Service to our Customers

4. Our member companies provide a wide variety of credit to people and businesses, allowing them to obtain goods and services, and invest in assets, which would otherwise create unacceptable financial burdens for them. Sophisticated and responsible means of sharing information about customers make this possible. At one time, the only way of getting credit safely was to ask a bank manager, who would base his decision on direct personal knowledge of the individual and perhaps his or her family. If turned down, there was little recourse other than to the unsafe, unregulated market.

5. Things have changed, and very much for the better. The Government rightly encourages customers to shop around in a vibrant and competitive market. Consumers use new technology, like the internet, to do so. They have greater choice, faster delivery, lower prices, constant availability, and a degree of anonymity that many people welcome.

6. But the new market brings its own challenges. The first is that, in the absence of the kind of direct personal knowledge available to lenders in the past, the credit industry needs another way of knowing its customers, so as to make sensible and responsible decisions about lending. And the second is that criminals will seek to exploit any weaknesses in this new market.

Benefits v Concerns

7. Data-sharing allows the industry to prevent over-indebtedness and to detect and investigate financial crime, including fraud, identity theft and money-laundering. For these reasons, it is widely supported by consumer organisations including *Which?* and the Consumer Credit Counselling Service. Any new barrier to responsible data-sharing would raise prices, reduce the availability of credit and increase financial exclusion, while making life easier for fraudsters and money-launderers.

8. The industry's CIFAS fraud prevention service therefore allows its members (the major banks, building societies, mortgage lenders, retail credit suppliers, finance companies, insurance companies, credit card companies and mobile phone suppliers) to exchange details of apparently fraudulent applications for credit.

9. Similarly, in the field of consumer protection, our data-sharing system relies on sharing with the Credit Reference Agencies information which helps build a picture of the financial position of a prospective borrower. For example, our members use shared data to identify existing customers who have reached the "tipping point" at which affordable credit tips over into excessive debt. They can then take action to help the customer.

[13] *The Soft Cage—Surveillance in America* by Christian Parenti, 2003, Basic Books.

10. The system is highly automated, which helps reduce the scope for human error or prejudice in lending decisions. This is amply demonstrated by the experience of the banking sector, which has found that the use of automated credit scoring and data sharing has reduced the percentage of over-limit bank accounts from about 8% to about 2%, and the percentage of overdue unsecured loans from about 4% to about 1%.

Impact on Liberty and Privacy

11. When anyone applies for credit, they are told that the lender will carry out a credit reference agency (CRA) check and that, if the application is approved and an account is opened, the lender will share information on the person's payment behaviour with the CRAs. Anyone who is unwilling to have his or her data shared has the option of not applying for credit.

12. It is clearly vital that the subsequent data-sharing arrangements include the checks and balances needed so that data is only gathered for clear and responsible purposes, and in a manner acceptable to society. Bankers have of course a general duty of confidentiality. All consumer credit companies are licensed by the Government. FLA member companies are also subject to a binding Lending Code, which sets out good practice in making lending decisions.

13. There is then a robust set of controls ensuring that customers are always informed of the use to which personal data will be put, and that access to such data is restricted to those who have a legitimate need for it. The bedrock of this system is the Principles of Reciprocity, which govern the sharing of data to ensure that it is used solely to prevent over-indebtedness and fraud, and not—for example—for marketing. The Principles are overseen by the industry's Steering Committee on Reciprocity (SCOR) which maintains regular contact with the Information Commissioner's Office (ICO) and the Department of Trade and Industry (DTI). This arrangement is unique internationally, and one in which the industry takes considerable pride.

14. Work is currently in hand to bring all the relevant explanatory and documents and protocols together in one place, using clear and non-technical language, so as to make them more readily available to customers. We want to make sure that everyone outside the industry understands the robust governance arrangements we have.

The DPA

15. The individual citizen is also protected by the Data Protection Act (DPA). The FLA believes the DPA is a sound piece of legislation which protects consumers' rights. But we also think that more needs to be done to educate people about it, and to ensure effective enforcement. Widespread and effective training in the reasons for, and impact of, the legislation is essential. We welcome the work the ICO already has in hand, and we have suggested that the approach currently being taken in the field of financial education by the Treasury and the FSA may afford something of a model.

Public-Private Data Sharing

16. There is significant scope to reduce crime and over-indebtedness through public-private data sharing in a way that strikes the right balance with the need to protect confidential data, under the DPA. Where the Government has information that can help direct private sector efforts to deter money laundering, fraud and terrorist finance, it should be shared. A recent pilot exercise involving public sector fraud data and CIFAS (see paragraph 8 above) showed between 30% and 40% of the same fraudulent addresses. Similarly, lenders notify suspicious money laundering activity to the Serious Organised Crime Agency via Moneyweb, an electronic reporting system for those in the regulated sector. The Serious Crime Bill contains important provisions which will facilitate this kind of exchange, and we support them.

17. By the same token, it makes sense for public agencies, in certain restricted circumstances, to have access to private databases, although these do not hold the same volume of information as public databases. Examples include:

- Cabinet Office access for employment vetting.
- Police access for employment vetting for certain roles deemed by the police force to pose a relevant level of risk.
- Passport Service access to vet applications for passports.

In crime prevention terms, if used in this way, private sector data is a force for good.

18 June 2007

Memorandum by the Foundation for Information Policy Research (FIPR)

The Foundation for Information Policy Research is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We wrote the report for the Information Commissioner in 2006 on "Children's Databases—Safety and Privacy", which concluded that the proposed sharing of information on children was unsafe and in several respects unlawful. We have also been involved for many years in medical privacy, surveillance, forensics, and the economics of security.

We would like to make the following points:

1. The hard question is this: is there anything that the Government may not do to "catch Osama" or "save Maddie"?

2. There are actually some answers: the Government may not torture people, or go for more than five years without an election.

3. Unfortunately, the ban on torture is not backed by a prohibition on illegally obtained evidence. Such a law would also help deter unlawful surveillance. But the Government's response to illegal use of evidence has been to legalise it retrospectively (eg wrongly retained DNA samples).

4. Also, the "modernisation" of elections has seen a huge rise in corruption—not because of "online" elections but because postal ballots were made easy, and post (whether paper or electronic) makes surveillance by vote-buyers easier.

5. So is technology changing anything? Well, the huge reductions in the costs of data acquisition, storage and processing alone would cause more personal data to be collected and used. Are we headed for the 'age of perfect memory' in which forgetting is difficult or impossible?

6. There are universal issues and UK issues. The interaction between technology and privacy is of the first kind. Human intuitions are not a perfect guide to maintaining privacy, and technology continually magnifies the risks. Internet postings can't be unposted; the social cues that constrain face-to-face contact are absent; and search engines let us find information that would previously have remained buried in local files. As more embarrassing material about more people comes online, we need more tolerance, better regulation, or both.

7. Commercial data use also raises universal issues. There are strong incentives for firms to collect more data so they can price discriminate, target communications and assess markets. As the costs of collecting this data fall, the incentives for commercial surveillance become ever stronger.

8. Governments have been much slower to innovate, and the quality of policy debate is poor; few senior politicians are IT-literate, and traditional NGOs don't understand IT policy. So change has often been driven by scaremongering. From about 1995 to 2001, empire-builders' favourite mantra was child protection; since 9/11 terrorism and hate speech have been added.

9. But the underlying issues are not new. The Home Office slogan "If you've nothing to hide, you've nothing to fear" does not justify blanket Internet surveillance any more than it justifies warrantless wiretapping or room bugs. Most people have things they wish to keep private at some time in their lives. So long as there are prejudices, this will continue—online or offline.

10. A serious case of inept use of surveillance data was Operation Ore, where over 4,000 men were raided on suspicion of child pornography, and it turned out that half of them were simply victims of credit card fraud. Thanks to the scaremongering, prosecutions continued even after problems started to emerge; many families were damaged and over 30 men killed themselves, some of them innocent. Innocent men were also driven to plead guilty after evidence critical to their defence was withheld. This disaster occurred in great measure because the state sidestepped a number of the controls we have evolved since the 13th century. The lesson is that technology should not lead us to abandon constitutional controls, but to reassert and strengthen them.

11. A further surveillance issue is equality of arms in both criminal and civil cases. The police have little difficulty getting CCTV files or ANPR data to prove your guilt; you have much greater difficulty getting them to prove your innocence. A bank can get CCTV images to prove that you made a disputed card transaction; you cannot get images to prove you didn't.

12. So how can we go about refreshing constitutional ideas for the information age?

13. At the level of philosophy, human rights are most commonly founded on the principle of human dignity. Pervasive surveillance will undermine personal dignity, and ultimately support for human rights.

14. There are other theories. A communitarian view is that many public goods depend on social capital—the networks of mutual obligation, reciprocity and trust that exist in society. Diminished social capital increases crime; damages child development; and particularly harms the poor, who have less human or financial capital as a backstop. Social capital is generally built by local action and diminished by central action: involving parents in running a school is vastly preferable to using a government computer as their surrogate.

15. A third view is that privacy is an internalised version of territoriality and serves to order society. This comes from the substantial research literature on the economics of privacy,[14] in which central problems are why privacy remains more of a luxury good than a fundamental right, and why people do not complain more about privacy erosion. We tend to the view that they are starting to, as awareness spreads from the policy and technical elite to the masses.

16. Both commercial and government surveillance impose significant costs on citizens. The former leads to social costs associated with ex-directory numbers, call screening, etc; the latter erodes trust in public-sector professionals as well as imposing direct compliance costs.

17. Yet in the UK, all this is ignored. The NHS is trying to centralise all medical records; other governments merely encourage hospitals and GPs to exchange data when needed. DfES plans to share data on children between the NHS, police, school and social work systems. We have a huge ID database project. These ventures appear to be driven less by any clear vision of how to improve services, as by a desire to appear "modern" (and in the case of ID, "tough"). The current Whitehall status game seems to be "my database is bigger than your database".

18. The FIPR report on Children's Databases found that the proposal to share most public-sector data on children was contrary to European human-rights law and data-protection law. The Data Protection Act does not implement European law properly in this respect. For the analysis and argument we refer the Committee to our report, especially chapter seven.[15] In summary, sensitive data can only be shared with consent or by law specific enough for its effects to be predictable by data subjects. Many of the laws relied on are so broad that their effect is not predictable. The consent provisions are also defective. For example, the *Gillick* and *Axon* cases established that when children aged 12–16 are asked for consent, their parents should normally be involved; the DfES has rewritten this into "Frazer competence" (not even spelling Lord Fraser's name correctly) and a doctrine that children should consent on their own—typically in schools, where they are expected to obey adults.

19. In addition to the proposed systems, some existing initiatives—such as the recent Ofsted study of 10-year-olds—appear to be clearly unlawful.

20. These problems are not limited to children's databases. For example, the Wilkinson case has shown that people who refuse consent to data sharing may be denied NHS treatment. It can be strongly argued that such consent is coercive and the new NHS databases are therefore unlawful; this is another point of conflict between UK Government policy and European law.[16]

21. Our existing constitutional rights are being violated but there is no enforcement that works. There is little public action, as the Information Commissioner's Office was designed to be weak: he is highly resource-constrained; he does not support a rights-based approach; and he will only enforce UK statute law, not European law. There is little private action, as UK rules on costs mean that individuals or NGOs who sue risk bankruptcy. This is in sad contrast to the vigour of the USA.

22. In conclusion, our government has rushed to embrace surveillance without really working out what the technology is good for. In the process it has found ways to sidestep or ignore constitutional restrictions, when these restrictions actually need to be refreshed – and worldwide may increase slowly in the medium term, for example with a broader digital statute of limitations.

23. In the short term, Britain's basic provisions are fairly sound: the problem is enforcement. In the absence of any realistic prospect of public enforcement, we urge the Committee to consider options for private action. A change to US rules on costs might just be the innovation that reinvigorates the British constitution. Then NGOs like FIPR would be better able to take action against the most egregious violations of privacy and other rights.

8 June 2007

[14] See for example http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

[15] *Children's Databases—Safety and Privacy*, Foundation for Information Policy Research, Nov 2006; at www.ico.gov.uk and www.fipr.org

[16] See Professor Douwe Korff's oral testimony to the Health Committee Inquiry into the Electronic Patient Record.

Memorandum by Tarique Ghaffur CBE, QPM, MA, Private Office of Assistant Commissioner

I understand that the scope of the Committee's inquiry is to explore the constitutional implications of developments in relation to the collection and use of surveillance or personal data. This will undoubtedly produce a variety of views around the privacy of citizens and their relationship with the state. However, the purpose of my submission is to focus more specifically on the surveillance and data collection issues in relation to the security of the 2012 Olympic & Paralympic Games in London.

On the 6th of July 2005, it was announced that London had been successful in its bid for the 2012 Games. Just 24 hours later 52 people were murdered in four terrorist attacks on London, which changed the security landscape overnight. The events of that day and subsequently on the 21st July, together with recent and ongoing counter-terrorism operations, have resulted in a threat level that continues to be severe. Equally, there is little prospect of any abatement in this situation, as the threats from global and home-grown terrorism, allied to organised crime, continue to be of serious concern. As a consequence, the issue of security and public safety has to be a primary consideration in all aspects of Olympic planning.

Security Approach

In 2006, the Home Secretary appointed me as the Security Co-ordinator for the London 2012 Olympic & Paralympic Games, on behalf of the Commissioner of Police of the Metropolis. My role is to co-ordinate the activities of 24 different agencies, including Emergency Services and law enforcement, in order to ensure a safe and secure Games.

To date, I have produced a security approach that is working towards delivering on five complementary themes: physical security, people security, capability building, operational readiness and legacy. My approach to security planning is based on three main principles: a defined security footprint; an end-to-end process that maximises the security opportunity whilst being proportionate; and developing the plan through partnership and consultation.

During the consultation process with our partners, stakeholders and customers, one fundamental issue that has arisen is the use of technology and data systems to support our security and safety approach. This discussion has not been confined simply to the collection and use of data, but also included issues in relation to intrusion, privacy and proportionality.

This subject is not new territory for the police service, as there is wide usage of CCTV, whether in the policing of town centres, sporting and ceremonial events or the 'ring of steel' around the City. Equally, the police make use of a wide range of data from third-party sources in our intelligence and information systems. This has to be set against the proliferation of private surveillance and databases in recent years.

However, while the police are already subject to strict regulation, this is much less apparent in the private arena. The police are subject to an existing structure of formal judicial oversight and consultation in relation to both overt and covert surveillance, as well as a comprehensive system of checks and balances around data protection and freedom of information legislation. This is a process that is very close to the heart of UK policing and one that remains central to the ethos of Olympic security.

Scale and Complexity

In order to appreciate the security requirement, it is important to have an understanding of the sheer scale and complexity involved in putting such an event together. In addition to the 10,500 athletes attending, there will be around 15,000 construction workers and 250,000 accredited persons, together with an anticipated nine million ticket sales for 33 competition venues across the United Kingdom. There will also be a significant number of VIPs attending the Games. Collectively, the issue of scale and complexity will present a number of challenges, particularly around the physical and "people" security of the Games.

Physical Security and Safety

As part of our commitment to providing a safe and secure Games, there is a need to ensure that Olympic venues are safe environments. Should the UK threat level remain severe, then we will not be in a position to provide sufficient human resources to mitigate any such threat or risk and even if we could, such measures might be slow or cumbersome. We will therefore be reliant on technology to provide some of the capacity required.

Our approach to planning will be therefore be to ensure that all the Olympic venues are "Secured by Design" ie that security considerations commence at the concept stage and are incorporated into the physical construction stage. We have learned significantly from the construction of other large projects such as the Millennium Dome, the Emirates Stadium, Wembley Stadium and Terminal 5 at Heathrow. Through "Secure by Design", we will be working closely with the construction industry around the introduction of visible security measures, including access controls, high-visibility policing and of course on-site CCTV.

It is important to note that physical security is not geographically limited to just the Olympic venues. If we are to provide effective physical security during the event stage, then we will need to extend the physical security to incorporate the whole of London. However, in order to widen this security perimeter we must maximise the use of existing technologies, such as CCTV and Automatic Number Plate Readers across a broader area, forming a London-wide technology footprint. This will support effective command decisions in relation to the Olympic policing effort across London. Equally, the value of CCTV in any post-incident investigation cannot be overstated, as the 7/7 and 21/7 investigations have demonstrated.

People Security

As stated above, the scale of people involved in both the pre-event stage and the event itself is massive, complex and challenging. During the construction phase, there will be a need for a database linking existing identity regimes with additional biometric identifiers of the people working both on and off-site, in order to validate identities. It is intended that these measures will assist in excluding unsuitable employees, as well as providing legality and legitimacy for any post-incident investigation that may be necessary.

In relation to the event stage, I am exploring how technology can assist in linking border entry, travel, accommodation and ticketing data, through the use of knowledge databases. This will undoubtedly require the availability of large amount of data, a significant proportion of which will be personal information. However, the use of such databases will enable us to identify security risks and put early interventions into place against a small minority of people, allowing a lighter touch for the majority at the venues themselves in the true spirit of the Games.

Proportionality

I am sensitive to the concerns that the public may have around any increase in the use of technology and data collection in relation to the 2012 Olympics. It is therefore important that we get the right checks and balances into place. Surveillance, and the subsequent impact on privacy issues, is a key concern of the public and has a clear impact on police-public confidence, which in turn goes to the very heart of policing in the UK.

However, it is important to remember that the police use of personal data and surveillance is already subject to extensive formal/regulatory oversight as well as internal inspection. Human rights considerations, including proportionality, form an integral part of the police decision-making process around overt and intrusive surveillance. The Olympic consultation process is also allowing us to present the case for technological need to a broad range of public stakeholders and capture their views. I would welcome any further views on any other arrangements that need to be put in place in relation to the 2012 Games.

Conclusion

The security effort around the 2012 Olympic & Paralympic Games requires the availability of data and surveillance to be effective. Equally, the new public/private partnership allows much easier integration to support the security approach. Any shift away from the current position around surveillance and data collection would seriously undermine the security and public safety effort, both in the run up to, and during the Games. I therefore ask that due consideration is given to the security of the Olympic & Paralympic Games in your deliberations.

8 June 2008

Memorandum by the Joint Council for the Welfare of Immigrants (JCWI)

The Joint Council for the Welfare of Immigrants is an independent, voluntary organisation working in the field of immigration, asylum and nationality law and policy. Established in 1967, JCWI actively lobbies and campaigns for changes in law and practice and its mission is to eliminate discrimination in this sphere. We are responding to this inquiry because a primary application of the collection of biometric data and data-sharing is the immigration control of non-EEA migrants.

The Application of Biometric Data Collection and Data Sharing to Immigration Control

Until recently the collection of biometric data had been restricted to pilot schemes applied to visa applicants from the so-called "high risk" countries a list comprising disproportionately poor countries from the global south such as Eritrea DRC, Sudan, Nigeria, Zimbabwe, Ethiopia, Cameroon and Ghana. By the end of 2006 this had extended to 42 posts. Currently the commercial partnership enrolment of UK biometric visas is being carried out but by the end of 2007 it is expected it will be applied at 150 posts and the strategic plan for the National Identity Scheme and Borders, Immigration and Identity Action Plan, published December 2006 assures us that by the end of 2008 that the collection of biometric data abroad will be extended to cover all visa applicants intending to travel to the UK. This in effect means half the countries in the world or all the non-EEA countries. In addition by the end of 2008 biometric documents will be introduced for non-EEA foreign nationals already in the UK who reapply to stay here.

It is anticipated that biometric data collection will be used not only to support the allocations of visas at overseas posts and immigration control at borders but will also be used to extend immigration control within the UK's borders. Biometric data and data sharing will be applied so as to mediate immigration control via access to employment (in conjunction with the illegal working sanctions contained in the Immigration, Asylum and Nationality Act and public services (for example via the overseas visitor rules for the NHS). In the aforementioned strategic plan at paragraph 19 it is stated that ID cards will be used to facilitate access to many public services: "This will be the case throughout the country, as the Scheme is UK-wide. Application, enrolment and the storage of data in the NIR will be managed on a UK-wide basis, in much the same way as passport applications operate today. However, the devolved administrations will have responsibility for how the ID card is used to gain access to those public services which are their responsibility."

This was reiterated in the Borders and Immigration enforcement strategy announced at the beginning of March 2007. Measures being introduced include a "watch list" of "illegal" migrants to alert government agencies if someone applies for services to which they are not entitled. For example there will be pilot schemes in three NHS trusts to be implemented by April 2008 using data from the Immigration and Nationality Directorate to ensure non-eligible migrants pay for non-urgent health care where required to do so. Offering justification for this approach the Home Secretary John Reid said most people who came to the UK wanted to comply fully with immigration laws but those who did not should not enjoy the same benefits and privileges. "This new approach will make life in this country ever more uncomfortable and constrained for those who come here illegally," the Home Secretary said.

JCWI's Concerns

We are concerned that the proposed collection, sharing and other uses of biometric data from disproportionate numbers of the non-EEA population before the mass of the UK national population in 2009 is discriminatory and will conflict with the UK's obligations under national treaties and conventions.

The latest Joint Committee on Human Rights opinion on the UK Borders Bill says it has not received sufficient information from the Home Office to ascertain whether the biometric data clauses are compatible with ECHR article 8. However in a previous opinion on the Identity Card Act it has said it considers the implementation of a compulsory scheme for non-UK nationals before UK nationals raises questions of disproportionate interference with private life under ECHR Article 8, as well as of discrimination under Article 14, read in conjunction with Article 8. In addition:

> "Further discrimination issues may arise, under Articles 8 and 14 of the ECHR as well as in relation to the UK's international human rights obligations of non-discrimination, in particular under the International Covenant on Economic Social and Cultural Rights (ICESCR) where essential services such as healthcare became dependent on entry onto the Register, for certain groups."

The technology is not foolproof. Already a major breach of privacy of biometric visas applicants has occurred in India following a system failure despite recent assurances given to JCWI by the UKVisas panel. A further example is the failure of systems to always properly match biometric data, The Government of Malaysia has recently admitted to wrongly expelling 400 migrants because of biometric data mismatches. It is not properly understood what the liability of the UK Government is in such instances but we note that while disclosure of such leaks is mandatory in the US in the UK it is not.

We believe that a culture of biometric data collection, sharing and checking of associated biometric documentation and registers, will inevitably result in, or amplify existing, discrimination against visible minorities in the UK. Research conducted in Europe has shown that that where such a culture of registering personal information and providing supporting documentation as proof of identity and lawful presence exists ethnic minorities are disproportionately checked. (Adrian Beck and Kate Broadhurst: Policing the

community: the impact of national identity cards in the European Union, Journal of Ethnic and Migration Studies, Vol.24, No. 3, 413–431, July 1998). This is also a concern of the JCHR in its recent opinion on the UK Borders Bill which considers that application of biometrical data collection for non-EEA nationals before UK nationals will lead to de facto carrying and production of identity documents by BMR groups. A further output for race equality that should be noted that BME groups are particularly prone to biometric data misreading and mismatching because as is the case with older people their irises and fingerprints are not as easily read by the technology and may in some cases be unreadable.

Legal opinion sought by JCWI advises that any power of public officials to demand identification including in relation to provision of public services, as mentioned by the national identity scheme strategic plan above at paragraph 19 will have a potential discriminatory impact not only on foreign nationals but also on ethnic minority British citizens who may be wrongly judged to be foreign nationals by officials. To deny health care or benefit because a foreign national does not have such documentation, without regard to his need, or to subject an ethnic minority British citizen to the type of enquiry contemplated in these clauses will most certainly fall foul of Articles 8 and 14 of the ECHR.

The Government has not acted ultra vires in restricting non-urgent healthcare to overseas visitors. Nevertheless additional opinion obtained by JCWI denial of non urgent health care may in specific circumstances give rise to human rights breaches associated with this denial under the ECHR, CEDAW and the UNCRC. This suggests that the collection and sharing of biometric data by giving rise to disproportionate breaches of privacy and by association discrimination, against foreign nationals may compound other breaches of human rights. They further compound the problems of risks to racial equality and effective monitoring associated with the Department of Health's failure to carry out a Race Equality Impact Analysis of the restriction of health services on which both the JCHR and the CRE have expressed concern. It is our understanding that the DoH is shortly to be the subject of a formal investigation by the CRE for its alleged failure to carry out this and its other statutory duties as a public body under the Race Relations Amendment Act 2000. It is therefore of concern if the Home Office believes the operation of the policy can be delegated to the devolved administrations without any direction as to the possible repercussions for race equality.

In addition in the course of the debate about identity cards and biometric data collection and sharing, very little has been said by the Government about assessing the public acceptability and impact on the public and third sectors and their employees of having to check and share biometric documentation and information and deny employment and services to those who have been living and working irregularly in the UK for many years and their children. The use, sharing and checking of biometric data to deny services so as to control immigration could also result in:

- individual employees code of professional ethics being violated;
- increasing administration duties for sectors which are already over-burdened;
- increasing destitution as services are denied with a resulting strain on third sector resources and advocacy;
- additional public health/acute services burden as people are discouraged from reporting health conditions in a timely way;
- increasing burden on public resources if the use and sharing of data results in increased detention and deportation;
- conflict in locations of public service provision such as hospitals; and
- and conflict with implementation of progressive equality cultures by public sector and the third sector.

June 2007

Memorandum by Dr Hazel Lacohée, Group Chief Technology Office, and Dr Andy Phippen, Network Research Group, School of Computing, Communication and Electronics, University of Plymouth

Executive Summary

Evidence presented here is drawn from the Trustguide project (www.trustguide.org.uk), a collaboration between BT Group, HP Labs and the University of Plymouth, part funded by the DTI. The Trustguide project sets out to better understand the private citizen's relationship with online technologies through a series of focus groups—resulting in in-depth dialogue with approximately 400 UK citizens. Within the discussion, surveillance and data collection technologies featured heavily, in particular issues such as ID cards and centralised healthcare records.

Key findings related to the aims of the Constitution Committee are as follows:

- The private citizen has an opinion on these issues, formed through personal experience, shared experiences with peers, and the reporting of the mass media.
- They are tolerant of CCTV in public places, but are aware of the growth of such systems and this is less acceptable.
- They do not trust the reported reasons the Government give for greater surveillance and data collection.
- They lack confidence in the state's ability to manage large scale IT projects securely and effectively.
- ID cards present a further erosion of trust between the state and the citizen, and offer little personal benefit to the citizen.
- The communication of realistic restitutional measures in the event of breaches in IT systems engenders trust far more effectively than 100% guarantees of security.

Context

1. Trustguide was concerned with exploring issues of trust, security and privacy in ICT based applications and services with the general public through dialogue with citizens, facilitated via 29 discussion groups between September 2005 and October 2006. Our findings suggest that UK citizens are technology aware and have belief systems informed by a mix of mass media communication, personal, and peer experiences. The research shows we are at a tipping point of public acceptability of surveillance and data collection.

Observations

2. The range and quantity of surveillance and data collection by public and private organisations has changed the balance between citizen and state in that citizens feel less trusted and, as a result, are far more sceptical of motivation for collection and monitoring. In most circumstances individuals have the right and opportunity to choose whether to engage with a particular technology and this level of control is fundamental to acceptability, adoption and how, why and where such technologies are used. Public surveillance technologies and data collection, by their very nature, do not allow for any individual discretion in relation to choice and control or any resulting repercussions. Technological advances have made it increasingly easy to monitor citizen's daily lives and gather large quantities of data concerning individuals but citizens are distrustful both of the technology and need for government to gather, store and utilise their personal information. Such data gathering and storage is perceived as increasing individual vulnerability, particularly in relation to security and ownership of personal information. Citizens are aware that their data is valuable, and feel that it belongs to them. Central to the trust and engagement of technology is personal control and since this is not possible with surveillance technologies, it is not surprising that strong feelings were voiced in regard to such data collection and gathering. Specifically, the forms of surveillance and data collection that have the greatest potential impact on the increasingly delicate balance between citizen and state are those that impose on what is perceived as the private sphere of life and impinge on an individual's purse or health. This includes data concerning identity, biometric details, and monitoring of everyday movement and activities.

3. Any form of surveillance and data collection will be considered constitutionally proper or improper depending on the degree to which it has quantifiable benefits to its citizens and the state. Claimed administrative, security or service benefits are ineffective in convincing the individual of their need, particularly when it is perceived as excessive, irrelevant or covert. In terms of what constitutes "proper" surveillance and data collection, UK citizens are remarkably tolerant of CCTV but our findings suggest that this should not lead to government complacency regarding further measures. We found high levels of concern regarding what is perceived as increasingly heavy surveillance of day-to-day movements and activities. State claims and justification for current and increased levels of surveillance (eg control of terrorist activities, reducing crime, road user monitoring) were greeted with scepticism both in terms of a genuine need for such high levels of surveillance and any evidence that it serves the stated purpose. This decreased confidence that it was for the benefit of society at large. Many citizens feel that their constitutional rights are being eroded in the name of security, yet few feel under the degree of threat that might warrant such measures.

4. Our findings suggest there is a line that should not be crossed and that we are very close to that point—the blurring of the boundaries between the private and public sphere of life. The quantities of electronic data held about individuals and the purposes to which that might be put now or in the future are of great concern to citizens. For example, in the groups we introduced the concept of ID cards as an aid to security and a means of easily identifying or authenticating oneself; however discussions developed around the theme of increased

vulnerability rather than security. This vulnerability was two-fold; there was an extremely high degree of scepticism that any data that is held electronically can ever be secure, and the enormous potential for "function creep" in use of data collected. Very few attendees thought that ID cards would aid either their personal or the nation's security and concerns were centred on Government's ability and reputation to hold data securely. Certainly the Government's reputation to deal with large IT projects, and the high profile reporting of such in mass media, contribute to the mistrusting nature of the citizen. Attendees were not averse to carrying a card in principle, but in practice many interpreted this as evidence of Government's lack of trust in its citizens and felt that this would be detrimental to, and change the balance between citizen and state irrevocably. In order to increase public confidence and trust in such a scheme tangible benefits serving both individual and public interests must be in evidence and the risks, implications and impact associated with potential abuse, unauthorised access to and/or use of personal information need to be carefully managed and this management needs to be open. Assuming that it is always possible to breach security, achievable and honest guarantees and effective fallback mechanisms need to be in place that cause minimum disruption to the individual and make restitution to victims. Guarantees of 100% secure, "unhackable" technologies are met with scepticism by citizens who, even if having no personal IT expertise, have been exposed to increasing reports in the media demonstrating this to be untrue.

5. The highest levels of resistance to ID cards concerned the possible addition of biometric data. Some biometric data gathering has more public acceptance than others. Fingerprinting is the most acceptable but is context specific; holding fingerprint data on an ID card might be acceptable, but fingerprinting at airports was considered excessive, and fingerprinting children in schools was considered unacceptable by many. Iris recognition raised concerns about risks following repeated readings and possible eye damage although speed and minimal invasiveness might impact on acceptability. Biometric data is considered to be intensely personal, belonging to and extremely valuable to the individual. Given its value, biometric data is also perceived as highly vulnerable to misuse. We also found that increasing police powers that legitimise the taking of fingerprints and DNA of anyone arrested, whether or not they are charged or found guilty of any crime seriously impinges on perceptions of civil liberties and undermines public trust. If such operations continue it is unlikely that biometric data will win widespread public approval and acceptance as a means of identification in common, everyday situations or as a means of access to public services. Whist no in-use technology currently uses DNA, our study revealed that this depth of biometric data gathering is considered the most unacceptable and strongly resisted by our subject groups. They are aware that DNA is more than a simple identifier—it has the potential to provide far more information about the individual and, as such, the citizens are extremely protective.

6. In relation to the storage of biometric information, another key issue affecting the trust of such systems arose. There were subsections within many groups that were uncomfortable, not from the privacy issues but because they felt if the Government had ownership of that data, there might be temptations to sell such information to interested bodies, as has occurred with DVLA data.

7. Increased public and private data collection and surveillance are changing the character of citizenship in relation to the state. Our research shows that many feel that this is detrimental to societal values because it diminishes individual responsibility for obeying the law, infringes civil liberties and personal freedom and reduces the private sphere of life to something that is quantified, measured and controlled by the state. Since personal information is collected and held outside as well as within the UK it is beyond the control of any UK legislation. A variety of measures need to be put in place that address individual and institutional rights, responsibilities and accountability and take account of the diversity of aims and motives in limiting, gathering and processing personal information. Our discussions showed most citizens were aware that the Data Protection Act could offer some protection but could not help them in dealings with entities outside of the UK and although increased legislation might be a partial answer many recognised that this would have to be a worldwide rather than national solution.

8. There is a clear requirement for greater individual control over how personal data is collected, stored, amalgamated and used, and a need for greater transparency of access to that information by the individuals concerned. It is also imperative to balance the removal of barriers to information access with new measures being implemented in response to contemporary security concerns. Since data relates to individuals many felt it is a basic right to know what information has been collected, how it has been used, combined, sold, which entities might be holding that information, how securely it is held and who has access and under what circumstances.

Conclusion

9. Given the current political climate it is of course difficult to strike a balance between national security and the maintenance of civil liberties. If technologies continue to be developed and employed with the intention of monitoring large numbers of people they are likely to intrude increasingly into the lives of ordinary, law abiding citizens who in turn will increasingly find cause to object. It is therefore imperative that surveillance technologies gain increased levels of public acceptance and to achieve this they should be deployed in a responsible manner, under strict supervision, and with increased levels of public accountability and individual rights of redress for mistakes. This should be supported by a legally enforceable code of conduct and regulations, and clear explanations as to the proven benefits and advantages of current and/or increased levels of public surveillance and data collection.

6 June 2007

Memorandum by the Law Society of Scotland

Introduction

The Law Society of Scotland ("the Society") welcomes the opportunity to comment on the House of Lords Constitution Committee's inquiry into the impact that Government surveillance and data collection has upon the privacy of citizens and their relationship with the State.

General Comments

The Society is of the view that, with regard to both surveillance and data collection, there clearly has to be a balance struck between the entitlement to operate surveillance and collect data as against the individual's entitlement to privacy, this being the issue that the House of Lords Constitution Committee will ultimately be required to decide upon.

In arriving at this decision, the Society would highlight what is perceived at the moment as an ever increasing move towards something of a "Big Brother State" where the United Kingdom is now the most intensely monitored country in the world and, according to surveillance experts, there are 4.2 million CCTV installed around the country, equivalent to one for every 14 people. Accordingly, surveillance of any form should not increase further without strong justification for it. A strong concern of the Society is that there would appear to be no published evidence that the increased use of surveillance and data collection has resulted in an increased detection of crime and conviction of criminals and a decrease in the commission of crime.

This evidence is required in order that the purpose of surveillance and data collection can be properly assessed.

If it can be demonstrated with statistics that it has led to both increased detection and conviction and decreased offending then, no doubt, the public would be more comfortable with the concept. The Society notes that, in a report issued earlier this year, the Royal Academy of Engineering warned that increased monitoring of society actually risked provoking a breakdown in trust between individuals and the State, eventually causing more harm than good. The Society would also highlight that technological advances have resulted in an increased unauthorised circulation of data, contrary to the Data Protection Act 1998. In this regard, there are clearly issues with regard to individual's having access to justice and the availability of effective remedies where data protection is breached.

Specific Comments

Theme 1—*How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and State in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

The Society is of the view that, as stated above, these questions cannot be answered without evidence which presumably is held and which the Constitution Committee should access. Undoubtedly, in any town or city centre, after the installation of security cameras, there will have been market research carried out to ascertain whether there has been any actual reduction in criminality. It may be considered that the increase in surveillance and data collection is a neutral development, issues only arising therefrom should the information fall into the wrong hands. It has been difficult to evaluate serious abuse but the concern here is the potential abuse of holding such information. Thereafter, the collection of data by private bodies is of greater concern

to the Society than the collection of data by public bodies as private bodies are not subject to the same level of scrutiny or requirements of transparency as public bodies and their aims may of course conflict with the public interest. The change in balance between the State and the citizen and the State in recent years is that many citizens may feel disempowered in relation to actions by State bodies. Many citizens feel the same way in relation to substantial private bodies as well. The Society would note that the extensive level of personal information held by State and public bodies is what will have the greatest impact on this balance.

Theme 2—*What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might the line be identified?*

The Society would suggest that if members of the public are to be surveyed, then the level of surveillance should extend only to the public arena. There may be some disquiet with regard to CCTV cameras in town and city centres but that could no doubt be considered constitutionally proper if it can be demonstrated that criminality is reduced. The Society would hold that a constitutionally improper form of surveillance would occur where the individual was being monitored outwith the public arena. The most obvious example being within his or her home where there is satellite surveillance, or a monitor of, for example, telephone or internet shopping. The Society feels that the bigger debate centres around the unauthorised passing of information from company to company leading to individuals receiving unsolicited junk mail and being subject to cold-calling. In general, this undoubtedly would have an effect on an individual's quality of life.

Whilst the Society considers that the individual being monitored outwith the public arena is excessive, it also considers that excessive use in general of CCTV, telephone tapping or the unjustified retention of DNA identification is constitutionally improper. The Society notes, however, that security considerations, such as a substantial terrorist threat or the prevention of serious crime can "move the line". There is a line not to be crossed but it is, accordingly, difficult to define. In essence, the balance is to avoid an overbearing diminution of the freedom of the individual and such liberties that should be curtailed, or breaches of privacy, should be limited to substantiated and significant issues of real public concern.

Theme 3—*What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

The Society feels that, with regard to the movement of information between organisations as stated above, that the individual's right to private life is gradually being eroded without a wider public interest of justification. Information is freely exchanged, often contrary to the Data Protection Act without the individual's knowledge. Potentially a very dramatic effect on liberty and privacy, however, is whether or not measures are justified in the context of an adherence to Article 8 of the European Convention on Human Rights ("ECHR").

Theme 4—*What impact do surveillance and data collection have on the character of citizenship in the 21st Century, in terms of relations with the State?*

In the absence of research available to it, the Society feels that it is not in a position to answer this question but notes that Government research may well have been carried out in order to determine whether the individual feels more secure and in touch with the State or otherwise.

The Society would question why, in all the circumstances, the State would consider it necessary to hold so much information in relation to its citizens.

Theme 5—*To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in the collection and use of surveillance or personal data?*

The Society is of the view that, without sufficient regulation, the Data Protection Act 1998 is ineffective against less scrupulous organisations which contravene the terms of legislation by illegally circulating information. It would appear that there are few, if any, prosecutions with regard to contravention of the Data Protection Act and it is, therefore, proving an ineffective safeguard against an individual's constitutional rights.

Theme 6—*Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

Yes, as stated above, the ineffectiveness of the Data Protection Act 1998 and the ensuing difficulties in prosecuting or sanctioning anyone who contravenes the Act would, in the Society's view, require a prohibition on the collection of information where it is being improperly circulated. This would also apply to CCTV surveillance where the use is unregistered and does not comply with the Information Commissioner's Code of Practice. This returns to the Society's initial view on the question of whether surveillance and data collection should be in operation at all, where it is neither strictly monitored nor properly held for a requisite period of time and thereafter securely destroyed, nor where, in general, there would appear to be no discernable benefit in its use.

The Society is also of the view that citizens should be advised in general, excepting always security considerations such as prevention of terrorism and prevention of serious crime, what information State or private bodies hold in relation to them and the reasons why they so do and that this is a right that should be enshrined in legislation.

Conclusion

The Society is of the view that, in the absence of the publication of any empirical research demonstrating benefit with regard to the use of surveillance and data collection, then it should fully endorse the House of Lords Constitution Committee's call for evidence.

June 2007

Memorandum by the London School of Economics and Political Science Identity Project

Executive Summary

1. This document presents an evaluation by the LSE Identity Project of key constitutional issues raised by the surveillance aspects of the Identity Cards Scheme, particularly as they relate to questions of effective Parliamentary scrutiny of proposals of this nature.

2. Its primary focus is on the idea of "enabling legislation" and "technology neutral" policy as illustrated by the Identity Cards Act.

3. As a result of recent events regarding the late production of the second s37 cost report and secrecy of the OGC Gateway reviews, we also present recommendations about these issues.

Summary of Recommendations

4. We recommend that the Constitution Committee look again at the role of "enabling legislation" for legislation with such a profound impact on the relationship between the individual and the State, as there is a strong argument for not leaving the detailed implementation of such Acts to secondary legislation and statutory instruments.

5. We recommend that the Constitution Committee look again at the role of "technology neutral" legislation, in light of the experiences with the Identity Cards Scheme.

6. We recommend to the Constitution Committee that, when future legislation proposes mechanisms similar to the s37 cost reports for the Identity Cards Scheme, any such mechanisms include details of the Parliamentary scrutiny such reports should initiate and details of any penalties that can be applied, should the will of Parliament be ignored, for example by late delivery of such reports.

7. We recommend to the Constitution Committee consider the ways in which Parliamentary scrutiny of major schemes can be enhanced through the effective use of Freedom of Information Legislation.

About the LSE Identity Project

8. The LSE Identity Project[17] provides ongoing research and analysis into the UK Government's proposals to introduce national biometric identity cards. The main Identity Project report[18] issued in June 2005 was over 300 pages long and identified six key areas of concern with the government's plans including their high–risk and likely high–cost, as well as technological and human rights concerns. The report received extensive,

[17] http://identityproject.lse.ac.uk
[18] http://identityproject.lse.ac.uk/mainreport.pdf

ongoing national and international media coverage, and was frequently cited during debates in both Houses of Parliament.

9. Since the publication of the main Report in June 2005, the LSE Identity Project has produced a number of further reports and cross–party briefings for key debates in Parliament and helped shape key amendments to the legislation, including issues of cost reporting and compulsion. Since the proposals became law in March 2006, the project has provided evidence for the Science and Technology Select Committee's review of the use of scientific evidence by the Scheme. Members have also analyzed information issued in autumn 2006 and spring 2007 about the ongoing costs of the Scheme as the government prepares for procurement.

10. Although initially focused on the UK proposals, the analysis presented by the Identity Project has also contributed to policy deliberations in related areas including the Federal Trade Commission policy process on identity management in the US, the Australian Access Card, and analyzing the policy landscape for identity policy in Canada.

11. Members of the LSE Identity Project have published and submitted a number of academic articles, including pieces in The Information Society, the European Conference on Information Systems and Communications of the ACM. Others are currently under review with other peer reviewed academic journals.

Enabling Legislation

12. Throughout the Parliamentary debate about the Identity Cards Act, Home Office Ministers emphasized the fact that the Bill was "enabling legislation" that would "allow" a system of identity cards to be introduced[19]. As a result, there is "much still to be done in terms of detail, regulations and all the other elements"[20].

13. As such, many of the details of the Scheme are not included in the Act, with these details being left to secondary legislation and statutory instruments.

14. The use of secondary legislation is not without its critics, as was acknowledged by the Home Office Minister Tony McNulty during the Bill's Committee Stages in the House of Commons: "I shall pass over what is in part a serious debate about constitutionality, secondary legislation and the 'Christmas tree' nature of enabling legislation"[21].

15. The role of secondary legislation was raised during the Parliamentary debates. For example, Mr Robinson noted: "Secondary legislation would be most unsatisfactory for dealing with changes in such an important measure. It does not give the House the ability to amend; we would simply be asked to accept, on a take-it-or-leave-it basis, any package that the Home Secretary might introduce"[22].

16. Mr Heath noted: "I accept that the Standing Committee process is, in many ways, a good means of examining the detail of a Bill—line by line—but it is difficult for a Standing Committee to perform the same role in respect of this enabling Bill. The process is thus imperfect and does not allow hon. Members to consider matters in depth"[23].

17. Perhaps the most direct criticism was given by Mr Garnier: "It is legislation by statutory instrument"[24] and as Mr Carmichael noted "The Minister may say, as he did today, that there will be 61 other occasions on which we will revisit the matter, but that ignores the manner in which secondary legislation is dealt with in the House"[25].

18. We recommend that the Constitution Committee look again at the role of "enabling legislation" for legislation with such a profound impact on the relationship between the individual and the State, as there is a strong argument for not leaving the detailed implementation of the Act to secondary legislation and statutory instruments.

Technology Neutral Policy

19. Another argument for "enabling legislation" is that it allows for what might be called "technology neutral" policy. Rather than specifying in legislation what technological measures might need to be put in place, this form of legislation allows for these details to be added at a later stage, including during the procurement process. For example, the final Identity Cards Act simply states that an individual may be

[19] eg Baroness Scotland, 19 December 2005 Column 1565
[20] Tony McNulty 28 June 2005 Column 1253
[21] 7 July 2005 Column 88, emphasis added
[22] 28 June 2005 Column 1204
[23] 18 October 2005 Column 717
[24] 18 October 2005 Column 804
[25] 18 October 2005 Column 805

required to allow "his fingerprints, and other biometric information about himself, to be taken and recorded"[26] rather than specifying the specific technologies that will be used by the Scheme. By not specifying that these biometrics must include face or iris recognition biometrics the Identity and Passport Service was able to lower the risks and cost of the Scheme by dropping the use of Iris recognition in the revised Strategic Action Plan[27,28].

20. In previous research[29] we have shown that attempts at technology neutral policy often face practical problems. Thus, issues associated with government access to email transactions change considerably when email is transmitted via the HTTP protocol (eg in web–based email systems like google mail and hotmail) rather than via the SMTP protocol (eg for "standalone" email systems). Similarly, very different data management approaches are needed to implement data retention policies for 'always on' broadband services compared to dial–up connections.

21. The Identity Cards Act further confuses the distinction between technology neutral legislation and legislation with specific design implications in the role of the National Identity Register[30].

22. Thus, whilst the Act does not specify the form of biometrics to be stored by Government, it does specify that the Secretary of State "establish and maintain a register of individuals" that includes "information about occasions on which information recorded about him in the Register has been provided to any person" (ie the audit trail). It also specifies other audit details that are recorded on the Register including: the date of every application by him for a modification of the contents of his entry; the date of every application by him confirming the contents of his entry (with or without changes); particulars of every occasion on which information contained in the individual's entry has been provided to a person; particulars of every person to whom such information has been provided on such an occasion; other particulars, in relation to each such occasion, of the provision of the information.

23. As can be seen, this is a very detailed "design specification" for the Scheme and its operation. Whilst nominally technology neutral it actually implies a very particular way in which the Scheme would be used in practice. For example, it strongly suggests verification against the National Identity Register for confirming someone's identity (rather than, for example, verification against the card[31]).

24. We recommend that the Constitution Committee look again at the role of technology neutral legislation, in light of the experiences with the Identity Cards Scheme.

Effective Deliberations about the Cost Reports

25. One of the key aspects of the Parliamentary deliberations about the Identity Cards Bill arose around the likely costs of the Scheme[32]. As a result of these deliberations, the Government accepted an Amendment from Mr Dobson calling for six monthly cost reports. We reviewed the reasons for the introduction of the s37 cost reports in our response to the first cost report[33].

[26] s5 5(a)

[27] http://www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf

[28] More correctly, according to the Annual Report of the Biometrics Advisory Group "In the choice of biometrics, this implied setting facial and fingerprint biometrics as requirements but allowing suppliers the choice of whether to use iris biometric to comply with the required matching performance" http://www.identitycards.gov.uk/downloads/Biometric_Assurance_Group.pdf page 9

[29] Whitley Edgar A. and Ian Hosein (2005) Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. Telecommunications Policy 29(11), 857–874. (ISSN 0308–5961)

Hosein Ian, Prodromos Tsiavos and Edgar A. Whitley (2003) Regulating Architecture and Architectures of Regulation: Contributions from Information Systems. International Review of Computing Law and Technology 17(1), 85–97. (ISSN 1360–0869)

Hosein Ian and Edgar A. Whitley (2002) The regulation of electronic commerce: learning from the UK's RIP act. Journal of Strategic Information Systems 11(1), 31–58. (ISSN 0963–8687)

[30] We analyse the "surveillance by design" implications of the role of the NIR in our submission to the Home Affairs Committee inquiry into "A surveillance society?" http://identityproject.lse.ac.uk/LSE_HAC_Submission.pdf

[31] The UKIPS website gives an example of how the Scheme might operate in daily life emphasizing the verification against the NIR http://www.identitycards.gov.uk/how-idcard-daily-collecting.asp. In this example, Colin is picking up a parcel from his local courier office. "She asks Colin to enter his Personal Identification Number (PIN). By handing over the card and entering his PIN, Colin is in effect giving his permission for the company to check that the card is genuine and belongs to him. No other information from Colin's details on the National Identity Register (NIR) will be passed on to the courier company. Within seconds there is a positive response. This confirms that the ID card is genuine and is not registered as lost or stolen. Colin can now take both his card and his parcel. The assistant will keep the delivery note and record that the parcel has been collected. The company's computer records will retain a 'transaction reference number' from the identity verification service to show that the identity check took place". (Emphasis added). Interestingly, the Home Office design assumptions used by the DWP in October 2004 included an option for offline verification (ie against the Card rather than the NIR) http://www.dwp.gov.uk/pub_scheme/2007/apr/assumptions-040407.pdf

[32] For more details on this, see Whitley Edgar A., Ian R. Hosein, Ian O. Angell and Simon Davies (2007) Reflections on the academic policy analysis process and the UK Identity Cards Scheme. The information society 23(1), 51–58. (ISSN 0197–2243)

[33] http://identityproject.lse.ac.uk/s37response.pdf

26. Section 37 of the Identity Cards Act is very clear about the obligation to provide reports on costs to Parliament:

> 37 Report to Parliament about likely costs of ID cards scheme:
>
> (1) Before the end of the six months beginning with the day on which this Act is passed, the Secretary of State must prepare and lay before Parliament a report setting out his estimate of the public expenditure likely to be incurred on the ID cards scheme during the 10 years beginning with the laying of the report.
>
> (2) Before the end of every six months beginning with the laying of a report under this section, the Secretary of State must prepare and lay before Parliament a further report setting out his estimate of the public expenditure likely to be incurred on the ID cards scheme during the 10 years beginning with the end of those six months.
>
> (3) References in this section, in relation to any period of 10 years, to the public expenditure likely to be incurred on the ID cards scheme are references to the expenditure likely to be incurred over that period by the Secretary of State and designated documents authorities on:
>
> (a) the establishment and maintenance of the Register;
>
> (b) the issue, modification, renewal, replacement, re–issue and surrender of ID cards;
>
> (c) the provision to persons by the Secretary of State of information recorded in individuals' en-tries in the Register.
>
> (4) If it appears to the Secretary of State that it would be prejudicial to securing the best value from the use of public money to publish any matter by including it in his next report under this section, he may exclude that matter from that report.

27. The Act received Royal Assent on 31 March 2006. The first s37 report was issued by the Secretary of State on 9 October 2006 (the first day that the House sat, after the summer recess). Thus, according to the Act, the second cost report was required to be laid before Parliament no later than 9 April 2007 (six months after the first report was issued). The House rose for Easter recess on 29 March 2007 and returned on 16 April 2007. Thus, the report could have been issued before the House rose (on any date upto 29 March 2007) or shortly after the House returned (16 April 2007).

28. On 25 April 2007, the Junior Minister Joan Ryan gave a written answer about the costs of the Scheme, where she noted:

> Revised cost estimates have been published from time-to-time, for example, when the Identity Cards Bill was introduced to Parliament. During the passage of that legislation, the Government agreed to lay a report before Parliament every six months, which sets out the estimated cost of the National Identity Scheme for the coming 10 years.
>
> She answered a further question on costs on 30 April 2007, repeating the information that the total expenditure on the Scheme to the end of September 2006 was £58 million since the start of the 2003–04 financial year.
>
> On that same day, she also gave an oral answer in Parliament to a direct question about when the second cost report would be issued:
>
> > Dr. Vincent Cable: Will the Under–Secretary explain why the ID card cost report, which was due to be published a month ago, did not appear, even though the Government have a legal obligation to ensure its publication?
> >
> > Joan Ryan: The costs will be presented, as we are committed to doing, in the cost report, which will be published shortly and in the Identity and Passport Service annual accounts for 2006-07. The hon. Gentleman can rest assured that the report will be before him soon.

29. The report was finally issued on 10 May 2007, the same day as Tony Blair announced his plans to step down as Prime Minister. Opposition parties and the press questioned the timing of the issuing of the report as an attempt to "bury bad news".

According to The Independent:

> The Home Office said the delay was "not significant" and denied that the report had been postponed because of last week's council elections.

According to The Scotsman:

> A Home Office spokeswoman denied the delay claims. "The announcement has been in the diary … it is no secret", she said. "We have not been able to publish it exactly six months after the last one because parliament has been in recess. A delay of just four weeks is not significant when it comes over a 10-year period."

The Herald reported:

> Last night, the Home Office said 9 April, when the new ID costs were expected to be released, had fallen during Westminster's Easter holiday and the department had released the figures "as soon as we possibly could". The timing with Mr Blair's departure announcement was coincidental, a spokeswoman insisted.

30. In a later written answer, Joan Ryan said "I regret that the latest report on the estimated costs of the identity cards scheme was not published six months after publication of the first report as not all the contents could be finalized in time. However, it was published some four weeks after the due date, on 10 May 2007, by way of a written ministerial statement, and this short delay must be seen in the light of the 10 year period covered by the report".[34]

31. Two key issues thus arise from this experience: 1) Although the purpose of the s37 reports is to allow Parliament the opportunity "to stop" the Scheme if it is getting out of control, there is no formal mechanism for either House to review or debate the implications of the cost reports. It is not at all clear what action could be taken by Parliamentarians who were concerned about progress with the Scheme, as revealed by the cost reports. 2) There appears to be no mechanism for ensuring that the cost reports are delivered to Parliament on time.

32. We recommend to the Constitution Committee that, when future legislation proposes mechanisms similar to the s37 cost reports for the Identity Cards Scheme, any such mechanisms include details of the Parliamentary scrutiny such reports should initiate and details of any penalties that can be applied, should the will of Parliament be ignored, for example by late delivery of such reports.

Scrutiny of Technological Aspects of the Scheme

33. Since 2000, a key activity for ensuring that the procurement of large government IT projects deliver value for money has been a process known as Gateway Reviews undertaken by the Office of Government Commerce (OGC). These independent reviews are intended to check that the plans for the project are sufficiently developed. In the case of the Identity Cards Scheme, the Government repeatedly asserted that the Scheme had passed its various Gateway Reviews but refused to disclose the contents of the reviews.

34. The Information Commissioner, who regulates the Freedom of Information Act (FOIA), disagreed with the Government and concluded that, especially in the case of such an important scheme, the Gateway Reviews should be made public[35]. Rather than accepting this decision, the government took the case to an Information Tribunal. In May 2007 the Tribunal concurred with the Commissioner and stated that the ID Card Scheme Gateway Reviews should be released[36]. However the OGC has since announced that it is seeking a High Court review of the decision[37].

35. There are also press reports that Treasury officials are ordering the immediate destruction of Gateway internal documents[38] so that they might never be revealed.

36. Effective scrutiny of major government proposals is a requirement for good government. This is particularly so for large scale, technological systems. As Appendix 1 shows, the complexity of the National Identity Cards Scheme is such that it is likely to require ongoing, specialist scrutiny. By challenging the decision of the Information Commissioner and the Information Tribunal it is apparent that government is unwilling to provide opportunities for such effective scrutiny to take place.

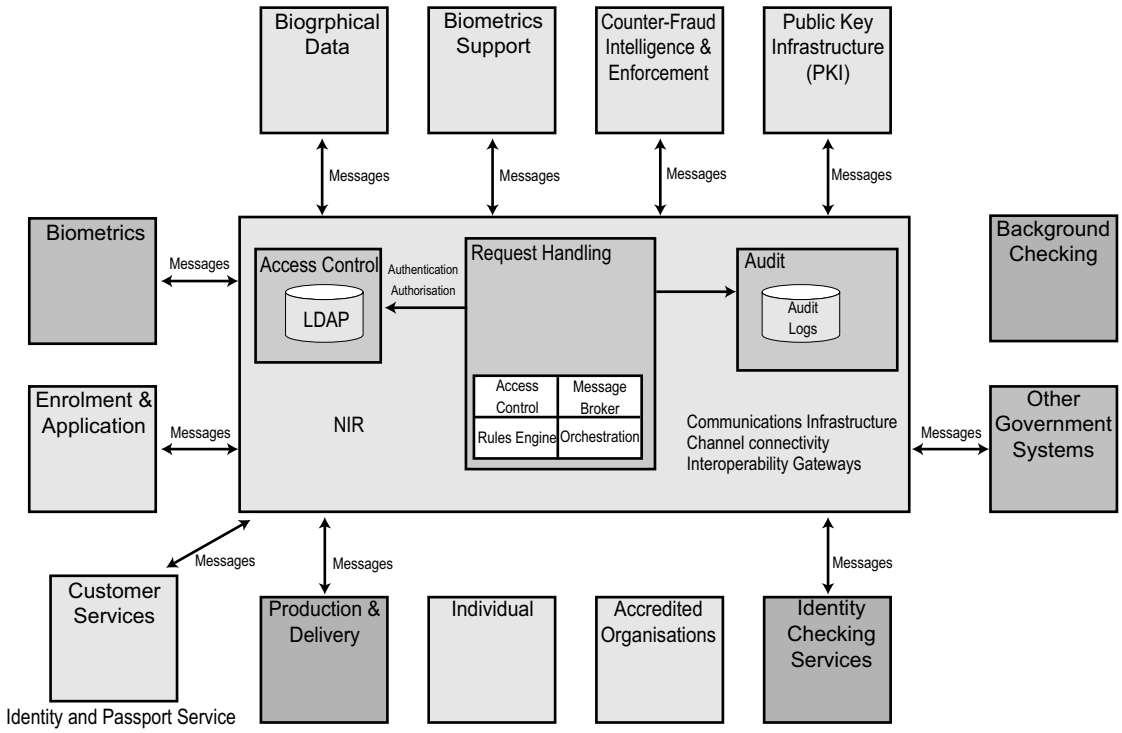
37. We recommend to the Constitution Committee consider the ways in which Parliamentary scrutiny of major schemes can be enhanced through the effective use of Freedom of Information Legislation.

12 June 2007

[34] Answer to question from Mr Hoban [136922]
[35] http://www.ico.gov.uk/upload/documents/decisionnotices/2006/decision_notice_FS50070196.pdf
[36] http://www.informationtribunal.gov.uk/Files/ourDecisions/office_of_govern_commerce_v_infocomm%20_2May07.pdf
[37] http://www.ft.com/cms/s/a633c624-0e4a-11dc-8219-000b5df10621.html
[38] http://www.computerweekly.com/Home/..%5C/Articles/2007/06/01/224487/civil-servants-told-to-destroy-reports-on-risky-it-projects.htm

APPENDIX 1

Presentation - Architecture (Level 1) - example
for Illustrative purposes



Taken from Feedback Presentation: Intellect Workshop: System & Programme Integration http://www.identitycards.gov.uk/downloads/2007-03-23Systems_and_Programme_Integration_Presentation_March2007.pdf

Memorandum by Dr David Moss, Director, Business Consultancy Services Ltd (BCSL)

Executive Summary

1. We prefer, in the UK, to be able to respect the government even if we do not always agree with them. In the evidence below, several examples are given of illogical behaviour by the government in connection with ID cards and ePassports. It is hard to respect an illogical government. And if respect goes, what will be next? Obedience? The government have set out, quite unnecessarily, on a dangerous path. This is a plea for them to turn back. For their own good and ours and as an example to other countries embarked on a similar course.

Credentials

2. David Moss of BCSL has nearly 30 years experience in IT and has spent over four years researching ID card schemes, with the following findings. Crime prevention, crime detection and counter-terrorism can best be assisted by making more use of the global mobile phone system, which we already have. ID cards and the unreliable biometrics which go with them would be of little assistance and even that would be delayed for years while we get the infrastructure installed.

Evidence

3. According to an April 2004 booklet[1] issued to UK employers by the Home Office, it is our responsibility to ensure that we offer jobs only to people who are legally entitled to work. The booklet includes a list of 18 documents we can use to establish that entitlement.

4. According to the Home Office's October 2006 cost report[2] on the ID cards scheme: "Currently, employers do not have a reliable means of establishing whether a job applicant has the right to work here or not" (p 5).

5. Logically, the Home Office could simultaneously believe neither of these statements, or just one of them, but not both.

6. The October 2006 report is at pains to say how hard it can be to identify people, not just for employers, but also for the criminal justice system: "It is difficult and resource intensive to ascertain the identity of prisoners suspected of being foreign nationals and those arrested by the police" (p 5).

7. And the problem does not end there. The Criminal Records Bureau Registered Bodies (CRBRBs) are no better off: "It is currently very difficult for [CRBRBs] to establish an applicant's identity efficiently . . . It is already known that on some occasions, individuals are matched against the wrong criminal record . . . this can lead to delays in processing their applications. In a small number of cases, people known to the police have been able to proceed through the system undiscovered" (p 5).

8. The solution to the identification problem proposed by the Home Office is biometrics (mentioned 41 times in their brief report): "Biometric checks and reduced reliance on paper documentation will help ensure that claimed identities are real, not fabricated or stolen. Each person registered will have a quick and secure way of proving who they are whenever needed, for example via a quick online match of their ID Card and biometrics or unique reference number. Individuals can only register once as their biometrics will be linked to a single identity, which will prevent the creation and use of multiple identities" (p 6).

9. Three biometrics have been considered by the Home Office—biometrics based on facial geometry, irisprints and fingerprints.

10. As far as facial geometry is concerned, the Home Office were warned four years ago[3] by the National Physical Laboratory that: "Face recognition on its own is a long way from achieving the accuracy required for identifying one person in 50 million" (p 11), "even under relatively good conditions, face recognition fails to approach the required performance" (p 15) and "facial recognition is not a feasible option" (also p 15).

11. Why, in that case, do the Home Office continue to give credence to biometrics based on facial geometry? Has something changed in the meanwhile?

12. It seems not. The Commissioner of the Metropolitan Police is quoted[4] in June 2005 as saying: "Identity cards are only going to work if we have a biometric answer—that may be iris recognition but it is unlikely to be facial recognition". And the National Audit Office (NAO) say in their February 2007 report on ePassports,[5] which incorporate biometrics based on facial geometry, that: "Facial recognition software is not reliable enough to use with large databases" (para 3.4).

13. As far as irisprints are concerned, the Identity and Passport Service of the Home Office have decided not to proceed with them[6] for the moment, citing "cost and technical uncertainties". At the same time, the Border and Immigration Agency of the Home Office are proceeding with irisprints for their eBorders programme[7]: "IRIS (Iris Recognition Immigration System) is a quick, convenient and secure way to clear immigration controls, open to British citizens, and foreign nationals with permission to enter the UK" (para 5.12).

14. How can the same technology be too unreliable for one bit of the Home Office while it is simultaneously acceptable to another bit of the Home Office?

15. Which leaves us with fingerprints. Most people are confident that traditional fingerprints are reliable. Rolled prints, taken by police experts using ink, are admissible as evidence in court. But this is not the technology being offered by the Home Office. Instead, they are offering flat prints, taken by putting your fingers on a photo-copier. This technology is different from traditional fingerprinting and is not admissible as evidence in court. It is something of a confidence trick to give the same name, "fingerprinting", to two such different technologies.

16. In the Home Office's evidence to the House of Commons Science and Technology Committee, reported in July 2006,[8] they acknowledged that flat print fingerprinting is not 100% reliable and stated that the maximum acceptable false non-match rate is 0.01 (para 18). By which they imply that if up to 1% of people find that the technology falsely reports that they are not themselves, that will be acceptable, but anything above would not be acceptable.

17. In fact, when the flat print technology was tested in the UKPS biometrics enrolment trial,[9] the false non-match rate was 19% (para 1.2.1.4). 19 is greater than 1. By the Home Office's own criteria, the technology is therefore unacceptable.

18. Instead of acknowledging this fact, the Home Office argued that the biometrics enrolment trial was not really a test of reliability: "When questioned in an oral evidence session about the false non-match rates that resulted from the Atos Origin trial, Katherine Courtney said that 'I think it is important to reiterate that the

enrolment trial was a trial of process and customer experience. It was not designed as a trial to look at performance of the technology *per se*' . . ." (para 88). In that case, why do Atos Origin list these performance figures in the *Management Summary* under *Key Findings?*

19. Given that this flat print fingerprinting is so unreliable, it is a consolation to discover that the UK, Ireland and Denmark are exempted from EC 2252/2004, a directive which instructs other EU countries to incorporate flat prints in their ePassports. That consolation is short-lived. According to the NAO's February 2007 report: "The UK is not obliged to comply with the EU regulations as it is not a signatory of the Schengen Agreement but has decided to do so voluntarily" (para 1.7). Why has the Home Office volunteered without debate to spend taxpayers' money deploying a technology which is known not to work?

20. Further, according to the NAO report: ". . . although there is spare capacity on the chip [in the ePassport] to store two fingerprints, the current model of chip has insufficient capability to accommodate the enhanced operating system and electronic key infrastructure required to protect fingerprint data" (para 3.14). So, in order to comply with this directive, which we do not need to comply with, to deploy identification technology, which does not identify people, at great expense to the taxpayer, we will have to recall the 2.2 million ePassports issued by September 2006 (para 2.1), and all the ePassports issued subsequently, and reissue them with bigger chips.

21. In his foreword to the November 2005 Cabinet Office paper on transformational government,[10] the Rt Hon Tony Blair MP, then Prime Minister, said: "But most of all we have to have the right people with the right professional skills to plan, deliver and manage technology based change". The examples above of illogical planning, delivery and management, suggest that we do not have the right people and that we should therefore abandon the ID cards scheme and the plans for transformational government based on them before any more taxpayers' money is wasted and before it becomes impossible to respect the government.

References

1 *Documents employers should use to check the right to work—Changes to the law on preventing illegal working: short guidance for United Kingdom employers*, April 2004, Home Office: IND Corporate Communications

2 *Identity Cards Act 2006—first section 37 report to Parliament about the likely costs of the ID cards scheme*, http://dematerialisedid.com/PDFs/costreport37.pdf

3 *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, Tony Mansfield and Marek Rejman-Greene, Version 3, February 2003, http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf

4 *ID technology "must be foolproof"*, http://news.bbc.co.uk/1/hi/uk/4095830.stm

5 *Identity and Passport Service: Introduction of ePassports*, National Audit Office, 7 February 2007, http://dematerialisedid.com/PDFs/0607152.pdf

6 *Iris use dropped in ID card plans*, http://www.itweek.co.uk/computing/news/2171789/iris-dropped-id-card-plans

7 *Securing the UK Border— Our vision and strategy for the future*, Home Office, March 2007, http://www.ind.homeoffice.gov.uk/6353/aboutus/Securing_the_UK_Border_final.pdf

8 *Identity Card Technologies: Scientific Advice, Risk and Evidence*, House of Commons Science and Technology Committee, 20 July 2006, http://dematerialisedid.com/PDFs/1032.pdf

9 *UK Passport Service Biometrics Enrolment Trial*, Atos Origin, May 2005, http://dematerialisedid.com/PDFs/UKPSBiometrics_Enrolment_Trial_Report.pdf

10 *Transformational Government—Enabled by Technology*, Cabinet Office, November 2005, http://www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf

4 June 2007

Memorandum by the Network Research Group, School of Computing, Communication and Electronics, University of Plymouth, Plymouth, United Kingdom

The evidence presented here is primarily in response to questions 2 and 3 of the call for evidence. However, it also presents data that demonstrates the need for the State to be responsible in ensuring it does not hold information on citizens in a manner that is susceptible to abuse. Data drawn from doctoral research into the impact of Internet technologies on the privacy of vulnerable groups shows the potential for harm in the event of information abuse. We would argue that any service provider or host holding citizen's data has an ethical responsibility to ensure that the information held is not open to abuse. We would suggest on the evidence we

have seen that this is not always the case with the State's storage and sharing of information. And as a result, the trust relationship between State and citizen is further eroded.

1. Evidence presented here is drawn from the Ph.D research undertaken at the Network Research Group, University of Plymouth, aiming to examine the potential impact of emerging web technologies on the privacy of vulnerable groups—while the scope of the research goes beyond a single group, the majority of evidence presented here is considers the experience of domestic violence Survivors.

2. In considering the response for the call to evidence, we would suggest this evidence provides contributions to questions 2 and 3 in that it examines cases where data held by the state has the potential for abuse, and the implications of that abuse on the private citizen. This, in turn, can harm the trust relationship between state and citizen. However, in addition, we would add that in considering how surveillance technologies and data collection impact upon the relationship between state and citizen, the evidence presented demonstrates the responsibility of the state to protect the citizen from the potential harm that can result from the abuse of data collected.

3. Technology is changing the way people communicate. The Internet is becoming an increasingly social space with many people choosing to interact with their peer group through social networking sites such as My Space and Bebo. Increasing numbers of mobile devices are able to interact in more depth with the Internet—the citizen is no longer limited to receiving emails on their mobile, they can now enjoy music and video downloads as well as browsing ability. Social interaction can be increased not just with texts and phone calls but uploading to online diaries from the mobile too.

4. Surveillance technology is clearly also on the rise. A recent report to the Government Information Commissioner by the Surveillance Studies Network[i] illustrates the growth in CCTV cameras—the BBC article "Britain is Surveillance Society" [2006] quotes it being one camera for every 14 people. Of course, all these technologies have legitimate uses and are useful in increasing safety.

5. However, our concerns lie in the fact that they can become tools of oppression when used by a perpetrator for violent or controlling means. The Internet has been identified as a tool for enhancing stalking behaviour[ii] and as a facilitator for the sexual exploitation of women and children[iii]. Technology is increasingly being used by perpetrators either for tracking people or to impose power and control. For example, there have been examples of Global Positioning System tracking devices that had been fitted to cars[iv] deleted emails that divulged important information utilised by perpetrators to track partners poised to flee; and websites divulging personal information and advertising sexual services or practices designed to either threaten Survivors or encourage others to contact, harass or harm them.

6. We acknowledge that this problem goes beyond the responsibilities of the state. Obviously the private sector—technology manufacturers and service providers—have a responsibility to ensure the technologies they develop do not have the potential for abuse, and that individual's private data remains so. However, in recent times, the state's reliance upon technology to support its own processes, and to deliver services to the citizen, means that there is a growing volume of public data collected by the government is increasingly available online; we see planning permission details, land registry data and civil registrations all available for small fees through the Internet. An increasing amount of information is being collected by the Government. For example, the Information sharing Index will have all children entered on the index by 2008, allowing all children to be tracked[v].

7. In carrying out research into the threats afforded to the individual as a result of emerging connected technologies, it was impact to understand the experiences of UK citizens and their perceptions of how data is collected, shared and managed by the state. Our research aimed to gain an in-depth understanding of how the privacy of Survivors is affected by Internet connected technologies. Exploring the different social contexts combined with the effects and influences brought about by third parties in a technologically mediated environment was identified as key to achieving this understanding. Various forms of data collection (semi structured interviews, focus groups, workshops) were employed to establish a dialogue with relevant parties, encouraging an open discussion rather than being led by specific questions.

8. Participants were selected by approaching statutory and voluntary sector bodies that worked in the field of domestic abuse. These included Probation Service, Police special Domestic Violence Unit, Refuges, and Women's Aid. These bodies were chosen to give a broad overall perspective, their representatives would have familiarity with the client group, have a broad experience of different situations that would be encountered during the course of their work, they would not be under intense duress and discussions with them would be less likely to cause more distress and danger.

9. An initial phase of discussion was for participants to consider the level of threat (high, medium or low) for various ICTs. The categorisation exercise carried out during the interviews highlighted concern over mobile phones, emails, third party databases, and public records. These were the areas considered to provide a high risk of danger—all those interviewed placed these in a high category.

10. Public records were a well known problem among participants. One respondent reported that survivors were advised not to enrol on the electoral register, even though the electoral roll allowed individuals to opt out of having their address publicised. The reasoning being that address information could still be obtained by visiting the local government offices. This tied in well with the findings from the stalkingsurvey.com[vi] who found that 17% of stalkers utilised information from public records for tracking.

11. Sharing information between agencies working with affected families has raised concern in previous work. The report for Women's Aid[vii] highlights the need for safeguards to ensure that details of a family are not used by perpetrators to track them down. The danger was illustrated when a standard report from a database was electronically transmitted to the perpetrator giving full details of the family concerned. 46% of respondents knew cases where contact procedures had been used to track down a partner. The issue highlighted here is that problems are caused by the way in which people are utilising the technology in an attempt to streamline their workload.

12. Another situation was described where a support worker was tracked to a refuge by a perpetrator accessing the UK Drivers Vehicle Licence Authority (DVLA) database. Measures had been taken to hide the location of the Refuge from the perpetrator and the Survivor felt some measure of protection through the anonymity. The Support worker had been mentioned to the perpetrator by name during various communications and this name was used to search the DVLA database accessed at his work to discover the drivers licence and car details. The occasion was described as a chilling moment when the perpetrator called the Survivor on her mobile phone, informed her of the number plate of the Support worker's car, described its exact location in the car park of the Refuge and gave the Support worker's full name and address.

13. Tracking refuges through their postcodes was acknowledged to be made easier with the advent of Google Earth, multimap.co.uk, aerial photographs, upmystreet.com and 192.com. Some people made use of Royal Mail PO Boxes to hide real addresses and were not aware that the Royal Mail allocates postcodes for PO Box addresses according to the address of the property, not the nearest post office. Certainly, the mapping of post codes to addresses is also a concern. In recent times refuge centres have started to appear in online mapping services, based upon their postcode[viii].

14. Our research has shown that citizens have good appreciation of the sorts of data collected by the State and are also aware of the potential for abuse. In some cases they have had experience, either first hand or through support networks, of the result of such abuses. Therefore, it is important for the State to recognise that it is not simply the management of such data that needs guarantees to engender trust from citizens. What is also very important is to be aware of the potential for abuse, and to provide the necessary infrastructure for protection and avoidance of abnormal use of such data. If such measures are not put in place, the concerns citizen's have about the abuse of their data could potentially further erode the relationship between state and citizen.

References

i http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf

ii Bocij, P, (2004), Cyberstalking, Praeger, Conneticut

iii Mitchell KJ, Finkelhor D, Wolak J, (2005), The Internet and family and acquaintance sexual abuse, Child Maltreatment, 10 (1): 49–60 FEB 2005

iv Southworth, C, Dawson, S, Fraser, C, Tucker, S, (2005), A High Tech Twist on Abuse: Technology, Intimate Partner Stalking and Advocacy, Violence Against Women Online Resources, Minesota, http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html

v http://www.arch-ed.org/issues/databases/IS Index.htm

vi Sheridan, L, (2005)., Key Findings from www.stalkingsurvey.com., University of Lancaster, date accessed 25/05/06

vii Saunders, H, Barron, J, (2003), Failure to Protect?. Women's Aid, Bristol.

viii For example, see
http://www.google.co.uk/maps?hl=en&cr=countryUK|countryGB&q=refuge&near=Bradford&radius=0.0&latlng=53793810,-1752461,14348105859932926414&sa=X&oi=local&ct=authority&cd=1

May 2007

Memorandum by Dr Daniel Neyland, Senior Research Fellow

1. I welcome the Committee's focus on state data collection and citizen privacy. I have carried out a number of research projects over the last 10 years which have focused on issues of privacy, surveillance and data collection in CCTV systems, airport security, traffic monitoring, assessment of household waste and, most recently, the proposed national identity card scheme.[39] These research projects suggest that the collection, analysis and mobilisation of information on the population in order to regulate and govern the population (whether through local, regional or national government), have consequences for the nature of relationships established between people and the state.

2. This research has noted three commonly articulated focal points for concerns with privacy: in relation to particular spaces (for example, the home), information (such as medical records) and bodies (which are often identified as the ultimate thing to protect). These three focal points are regular features of concern articulated across different discussions of privacy, across different research projects.

3. Many of the concerns articulated centre on a desire to be informed regarding any incursions made through perceived boundaries around the particular area of concern and what happens to information collected from those areas.[40] Invasion-of-privacy arguments can sometimes focus on the first part of this concern—incursions through boundaries to collect information—at the expense of the second part of this concern—the use and mobilisation of data which may take that data into the public realm. The continual use of CCTV footage on television reinforces this possibility for much of the population. I have suggested this concern is not so much about an invasion of privacy as an invasion of publicity.

4. Beyond being informed about data collection and use, in a minority of cases, research participants have also expressed a desire to play an active role in managing these incursions (ie they would like to dictate what is and is not acceptable in relation to data collected, analysed and mobilised). In many more cases, participants have expressed a willingness to delegate management of privacy to a notable (usually state or state sponsored) organisation who they assume will act on their behalf and protect their interests.

5. In the latter case, the same participants assume that this is the current state of privacy protection, with notable organisations already protecting the population's privacy in data management activities. At the same time, however, awareness of key features of privacy protection appear low, with only a few research participants able to discuss the principles of the Data Protection Act and no-one able to name the Information Commissioner.

6. It should also be noted that key components of the Data Protection Act depend on a model of the 21st century citizen[41] as a participative, informed, concerned individual who actively manages his/her own privacy and balances his/her surveillance relationship with the state through a knowledgeable assessment of that relationship. There are not many individuals who fit this model of informed concern and many individuals assume that state apparatus is not something from which they have to actively protect themselves.

7. In practical terms, this can be problematic. For example the Information Commissioner's CCTV Code of Practice provides an interpretation of the Data Protection Act for CCTV systems. This Code suggests CCTV systems should: publicise who is responsible for the system, how members of the public can get in contact with the system and provide annual reports to the Commissioner of issues raised in relation to the CCTV system. My research suggests very few people are aware that they are supposed to take an active role in managing their own privacy, have no idea how to contact a CCTV system, or what a CCTV system can do or is doing (and so have little basis for forming a complaint).

8. These problems are likely to continue and may even increase with the introduction of biometric identification systems. The population may not know how the system operates in detail (thereby making challenges to the system less likely), may not know they are supposed to be actively involved in managing their

[39] A summary of the ID card research can be found here: ID cards (http://www.sbs.ox.ac.uk/research/sci-tech/mundanegovernance/ID+Card+Research.htm) Other areas of research feature in a recent book: D Neyland (2006) *Privacy, Surveillance and Public Trust* (Palgrave-Macmillan, London).

[40] It should be noted that specific concerns regarding specific technologies are unevenly distributed with, for example, twice as many non-UK residents having privacy concerns regarding biometric ID cards as UK residents (in airport-based research).

[41] It should be noted that much discussion of state data management activities focuses on the individual as the principal matter of concern. However, age, appearance, group actions and skin colour can each form the basis for the development of categories of suspicion. That is, these collective attributes can be invoked as the justification for data management. It is not clear how this should operate in relation to the legislative focus on individuals' rights and responsibilities. Does there also need to be a complimentary focus on groups' collective rights and responsibilities? Who should be talking on behalf of these collectives and through what means?

own privacy (thereby making challenges to the system less likely) and may not be aware of the process they need to go through to hold the system to account (thereby making challenges to the system less likely).

9. This problem raises questions for the relationship between state and the population proposed by Data Protection legislation. The relationship built into the legislation is one of mutual accountability whereby the state holds the population to account and the population holds the state to account. The absence of active, informed and concerned individuals suggests that the state's data management activities are lacking accountability. Why, then, is mutual accountability such a central feature of privacy protection? What alternatives might there be to mutual accountability? Do these alternatives have greater prospects of success?

10. Mutual accountability is often heralded as the way forward in privacy protection policies on democratic grounds (that the population should be given information, access, rights to ask questions and so on). Mutual accountability may also appear attractive due to the low apparent cost of this form of accountability in comparison with, for example, systems of inspection (such as holding schools to account through OFSTED).

11. If one wishes to take accountability and the management of privacy seriously, the costs of mutual accountability need to be weighed against the benefits of alternatives. First, it might be possible to enhance the effectiveness of existing forms of mutual accountability by, for example, investing in more effective communications so that the population is aware of accountability opportunities, how to hold the state to account and how state funded systems (such as CCTV or biometric ID cards) operate. However, the current system of, for example, CCTV accountability appears inadequate, so there are no strong grounds for arguing this same system would work in relation to ID cards.

12. Second, it would be possible to hold state data management to account in a similar fashion to other areas of state activities such as schools or hospitals. This would require teams of inspectors, performance measures, benchmarks and league tables through which data management systems would be made aware of their own accountability and the population would be offered opportunities to assess the performance of state data management. However, such a system would require a far more significant investment than the first option and may just add to the burden of information which the population currently ignores.

13. Third, it would be possible to utilise existing government infrastructure and hold data management practices to account through an expansion of the Information Commissioner's office. This could feature selective, random, unannounced inspections of state funded data management systems, compiling and publicising result of such inspections and greater effort devoted to public education in privacy protection. This third option would be less expensive than the second option due to its emphasis on selective rather than blanket coverage. However, it would require a commissioner with teeth who could actively question government policy and challenge state funded data management practices. Combining inspections with innovative education initiatives would enhance both a formal system for holding state data management activities to account and accountability of the state by the population.

1 June 2007

Memorandum by NO2ID

This Submission

1. This submission has been prepared for NO2ID, the national campaign against ID cards and the database state. The inquiry addresses NO2ID's central concerns concerning the alteration of the relationship between citizen and state by database government, and we welcome the Committee's recognition of the very serious constitutional implications.

2. This is necessarily a very brief summary of the legislative and institutional context and contains some novel legal proposals. Though compressed, it is still rather long. We would welcome the opportunity to present such supplementary evidence, orally or in writing, as the committee wishes to take.

3. We have also made a submission recently to the surveillance state inquiry being conducted by the House of Commons Select Committee on Home Affairs. We have tried to avoid repeating ourselves though some of the issues addressed are similar.

About NO2ID

4. NO2ID (an unincorporated association) was founded in 2004 in response to the Government's stated intention to introduce the compulsory registration and lifelong tracking of UK citizens by means of a centralised biometric database. NO2ID seeks to put an informed case against state identity control to the media, to national institutions and to the public at large. More than 100 organisations, including trades

unions, political parties, local authorities and special interest groups have either joined or made formal statements supporting the campaign. More than 30,000 individuals have registered their support.

5. NO2ID is non-partisan, and neutral on most political questions. Our concern is the threat to privacy and liberty posed by mass surveillance, the collection, retention and collation of information that can be tied to individuals, whatever the ostensible or intended purpose. Information sharing or matching used to generate files on individuals without specific and reasonable cause and independent oversight is a special case of the broader problem.

6. We regard a loss of privacy or anonymity without good reason as potentially a fundamental threat to the free society. If you are being watched or followed over time by someone with the power to discipline you directly or indirectly, then your freedom of action is reduced. The more minutely and extensively you are watched, the greater the power of discipline.

7. NO2ID's approach is therefore that information on individuals (and implicitly, therefore, on their associations) should not be stored or transmitted without good reason and limited purpose.

Summary

8. NO2ID believes that the unconsidered growth of government data-sharing intitiatives, together with advances in technology have inadvertently brought us to the verge of a surveillance state in which every action of the citizen is potentially subject to monitoring, retrospectively via data searches more than contemporaneously after the manner of the traditional police state informer networks.

9. Latterly this tendency has been exacerbated by the deliberate policy of "joined-up" or "transformational" government, which perceives the citizen in terms of the manipulation of a personal file, and idealises an integrated total information awareness for government. Such ideas have been seen as so self-evidently good by those proposing them, that they have been willing to subvert basic principles to pursue the policies concerned. The Identity Cards Act 2006, whose prime function is the establishment of a central register of the population, is the key such measure, but not the only one.

10. Technological and institutional change has subtly undermined our suppositions about privacy in everyday life, which are taken for granted in the constitution almost as much as they are by ordinary people. In particular we are used to having anonymity and privacy (which are very closely allied and interchangeable for many purposes) by default. They can no longer be taken for granted.

11. The threats are novel, and therefore the existing legal protections for the citizen are not adequate (even where they are not being broken down by zealous expansion of government remit). We are open to the equivalent of searches without proper control. And we lack control over information about us once it is no longer secret.

12. The existence of a permanent personal record which can be increasingly referred to by others reverses the presumption of innocence and the trust on which our system is based. It threatens to become necessary to prove ones "clean" status constantly, and an innocent incident, once on a record, is liable to be interpreted as grounds for suspicion.

13. NO2ID therefore suggests that a more considered approach is adopted in which promiscuous data-sharing is anathema rather than the ideal, and pseudonymity and anonymity are protected. Some specific measures ought to be repealed, but that is insufficient without new controls on the technology and institutions of surveillance.

14. We look forward to searches of private data being treated in the same way as physical searches of people and property. We advocate the extension of personal rights in relation to private information, and in particular the examination better defined understanding of privacy and "informational privity" whereby the use made of personal data remains in the control of the individual.

Discussion

Growth of the database state is unconsidered

15. There is a naivety in many government statements about data-collection and data-sharing powers. There is seldom a case made that recognises the seriousness of the exercise. Powers of physical search have less profound effects on the individual and society (as discussed below) but they are frequently controversial. It seems to be a matter of unconsidered administrative convenience in most cases.

16. Surveillance measures, particularly database surveillance measures have become routine. They are added piecemeal by new statutes, which are habitually drawn extremely widely and provide for extension by statutory instrument. Drafting will often include a catch-all provision, in effect permitting arbitrary other use of information. This is calculated to allow powers to multiply, interact, and evade proper scrutiny.

Technology enables the surveillance state

17. Our way of life is predicated on the fungibility of most records and the limited application of others. Your business and personal relationships would historically have been with and through people, who have a limited capacity and desire to store and process information. Copying and transferring a document before digital means became available required human intervention (even to place it on a photocopier or fax), searching archives required human beings to set up indexes, and so archives were constrained to their original purposes.

18. It is the ready recording, retention, copying, searching and sharing of information in ways that are effectively permanent and outside the control of the individual concerned, that potentially alters the nature of all relationships mediated by, or observed through, technology.

Constitutional conception of the person

19. Our law and constitution have developed in the context of direct relationships between individuals and institutions. They generally answer the question, "Does this person have this right in these circumstances?" and deal with the nature and consequences of transactions between persons. It is the essence of the rule of law that different persons are treated the same in like circumstances.

20. The function of law has historically been to adjudicate between persons on factual matters. It has accepted the real world, and managed conflicts within it.

21. We suggest that the growing culture of state identification and record keeping is eroding that fundamental assumption of law. When the first question asked is "Who is this person and what is their record?" and the answers condition their rights and treatment, then something has changed.

Bureaucratic conception of the person

22. An alternative conception of a person is found in the Identity Cards Act 2006, and is also visible in much recent legislation and regulation.

23. First, persons are conceptualised as attachments of official records, and their rights as dependent on registration. The person has been supplanted by the record. It becomes questionable under such a regime whether the natural person is any longer a legal subject.[1] The completeness and procedural correctness of records is the primary consideration of a bureaucracy. The law strives to deal with uncertainty, bureaucracy to eliminate it.

24. Second, unlike the law, which seeks to determine what are the relevant grounds for decision and does not concern itself with other properties or capacities of its subjects, a bureaucratic framework implicitly requires one file related to one body for all purposes, so that the individual can be efficiently managed by the state. It is intolerant of the multiple roles of individuals, which society and the law built on society can sustain.

Transformational Government

25. The notion of "Transformational Government"[2] which takes a governmentalist viewpoint for granted, is not simply an attempt to use new technology effectively, but is built around the idea of breaking boundaries between departmental functions by collecting and collating information on citizens across the whole of government. The Department of Constitutional Affairs's "Information Sharing Vision Statement"[3] identifies the "barriers" to broad data sharing as human rights law, data protection, common law confidentiality, and *ultra vires*. There are already frequently explicit statutory provisions setting aside confidentiality[4] and or working around data protection legislation.[5] Those are not, we submit desirable. But the idea that *ultra vires* is dispensible is profoundly anti-constitutional.

26. Such an approach requires a means by which information on citizens may be readily cross referenced. There is power to do it created by very broad drafting of the Identity Cards Act 2006. The Government made great play of the use of the scheme being "limited" to the statutory purposes, but the statutory purposes happen to encompass any conceivable activity of any future government.

27. Since that legislation was passed, the government and the Identity and Passport Service have begun to refer to the "National Identity Scheme" and to "identity management". We note that a governmentalism in which the citizen is deemed to be under the state's management is also foreign to our constitution, which supposes the individual to be at liberty under the law.

The Loss of Anonymity and Surveillance

Authentication and Identification

28. Security analysts distinguish carefully between the authentication of transactions and the identification of entities, between having authority to do something warranted by appropriate credentials, and being a particular person.[6]

29. The law does recognise such distinctions implicitly (in the conception of office for example: the Secretary of State will be a different person at different times, but bear the same authority) but this basic conceptual framework seems to be unavailable to lawmakers and others when it comes to discussing how the individuals interact with the state. The promotion of the National Identity Scheme in particular has consistently blurred the distinction between authentication and identification, as if it doesn't matter. Making individual actions traceable to individual persons is the essence of surveillance.

Discrete transactions versus tracing

30. Everybody recognises that it is neither necessary nor desirable—indeed completely contrary to the point of money—for the Bank of England to have a record of every time a note it backs changes hands. The same ought to be "obviously" true for other civil transactions, where authentication of capacity is what is minimally required. Identification, on the other hand, makes our actions traceable, a contribution to a central file rather than discretely legitimate acts. This opens the door to discrimination between different persons in the same circumstances, and to subsequent retrieval of information about individuals.

Ready accessibility of records

31. It is implicit in much recent legislation that if information can be retrieved and there is a legitimate reason for doing so, then it ought to be retrievable, with the minimum of formality. We believe that this is a moral delusion arising from the relative ease and invisibility of such processes. If information is hidden to human inspection, because it cannot be discerned among other facts or because it cannot be collated and cross-referenced by a person, then it is to a human mind obscured, and remains private. Uncovering and collating personal information from numerous inadvertent events, may reveal things about individuals that they did not intend on isolated occasions to reveal (and it may give rise to unwarranted suppositions about the meaning of those events). An example might be collecting one's entire Google search history.

Irrevocability of information transfer

32. Peter Bazalgette, the UK producer of "Big Brother" recently made the interesting observation that people may be willing to give out information about themselves at one stage of life, but regret it later.[7] This is not a large problem in the human world—the number of people who can learn something directly is limited. But the same information in a permanent searchable form can haunt us for ever.

33. If Bazalgette's example of Facebook sites seems too trivial, consider the Department of Health's National Programme for IT. There patients are expected to give permission[8] once only and irrevocably for their medical records—or their children's medical records—to be uploaded to the "NHS Spine" system, regardless that they cannot possibly forsee, or grasp the social and emotional consequences of future medical events in their life. Someone at 40 may wish to withhold records containing past incident of mental illness or sexually transmitted disease from general circulation; how can the same person at 16 make the same decision beforehand?

Expanded Consent

34. Not only is consent in many cases illusory, but consent to information sharing once given can lead to total loss of control for the subject. It is commonplace for forms for public purposes to waive data protection in effect, while being in practice impossible to decline to fill in. Most committee members will have an example to hand in the "security" forms for attendees at party conferences, where the extensive personal data provided is typically not limited to use for the event, but may be used for any police purpose.

Limitations of Current Protections

Privacy

35. Though we are accustomed to refer to it, there is no clear legal conception of nor direct protection of privacy *per se* in this country.[9] The US courts have, controversially, managed to interpolate a substantive right of privacy[10] into a Constitution that has none explicitly. This can be explained by noting that until recently no means were available to monitor and record people's activities at a distance or without permission on their own premises. At common law privacy was assured so naturally as a consequence of property rights that no-one thought to separate the two.

36. We note that what is often referred to as a "privacy" provision in the human rights convention received into our constitution in the Human Rights Act 1998, Article 8, the "right to respect for private and family life" (1) is not really a privacy provision since it accords a rather vague respect, not privacy itself, and (2) is subject to broad exceptions open to the state to adduce.

37. There is a case for creating freestanding privacy rights that cannot be readily abridged by the state without specific cause.

Confidentiality

38. The nearest we have to privacy law in Britain is arguably the law of confidence. There are problems with this, however. It is increasingly identified with the protection of commercial interests,[11] and it needs to be vigorously pursued because once information is public knowledge it can no longer be protected. Enforcement is also a problem; it requires that the leak be traced back to source, so that breach of confidence can be established, and the main means of enforcement is risky and expensive injunction.

Data protection

39. In our view the Data Protection Act 1998 is utterly inadequate to the purpose of protecting individual privacy and liberty against the surveillance. Most obviously Part IV of the Act provides effective exemption for government use of data for many purposes, and can readily be extended. Further it relies on compliance with regulation and guidance not prevention or individual remedy. The Office of the Information Commissioner relies on state funding, and already has great difficulty coping with the amount of work placed before it.

Consequences of Data Surveillance for Civil Liberty

Presumption of guilt

40. Where one is required to demonstrate a legitimate status in order to perform civil functions[12] then that imports a presumption that anyone who does not do so willingly is a suspect. The Home Office itself suggested as much in its "Benefits" paper for the ID scheme in 2005.[13] Once there are records to be disclosed they are subject to interpretation, which also may import presumptions, particularly in conditions designed to encourage suspicion. One clear example is of the existence of a record on the national DNA database, which implies prior arrest, which may be prejudicial in investigations.

Self reporting

41. The idea of continuous self-exculpation is aligned with the pragmatic consequence of surveillance mechanisms. The records must be complete. Therefore they must be kept up to date. Therefore the citizen acquires new and onerous obligations backed by penalties for non-compliance, to report on himself.

Abolition of rehabilitation

42. It may not be an articulated constitutional principle that an offender who has been punished is normally entitled to regard his debt as paid, but it is implicit in custom that people may escape their past. It has been persuasively argued by Simon Cole[14] that the idea of identity first came into use in criminal justice not for detection purposes, but because of the fear of recidivism. Where a conviction—or a mere social embarrassment—is permanently on record,[15] then we are fated to live in a harsh world.

Information sharing as a search power

43. As noted above (29), the identification of a specific act or transaction with a specific person is a disclosure about them beyond that strictly necessary and needs a reason. It is analogous to a police power of search. Currently police do not have the power to require information of people as to their identity or movements without suspecting them of an offence—and the recent suggestion that they might is highly controversial. Yet a data-sharing power granted to a public body doing precisely the same thing—identifying a person and his transactions—is so common that it is scarcely noticed. Because it is a power more easily exercised, ought we not be more concerned, however?

Data matching = general search

44. Matching or mining data is correspondingly more serious for privacy, as suggested in 30 and 31. If it is directed against an individual it is analogous to a police search. If it is used to draw conclusions from data-sets about groups, or to look for new patterns, then the only physical-world analogy is Writ of Assistance, which was sufficiently repugnant to liberty be outlawed by the US Bill of Rights, and survives here only as an unusual power of Customs Officers. Yet this is available *ad hoc* to the authorities under several pieces of legislation and the Serious Crime Bill, schedule 7 would create a general power in relation to the very broad category of fraud.

Recommendations

Repeal of Identity Cards Act 2006

45. The Identity Cards Act is designed around a conception of nationalising personal identity. It must be repealed. If identity cards themselves are justified (which we deny), then a system without a centralised register is entirely possible[16] and would not subordinate the individual to the state in quite the same way, but this would require new legislation.

Compartmentalised government

46. The "Transformational government" strategy, as currently conceived, is a direct threat to the rule of law and should be abandoned. This does not mean abandoning the use of technology for improving the efficiency of government activity; it means systems should be constrained to well-defined purposes.[17] We would prefer a compartmentalised government in which each department of state maintained a separate relationship with those citizens in its sphere. This is no inhibition to the coordination of policy, but is protective of individuals.

Recognition of privacy rights

47. In addition consideration should be given to new personal privacy and informational privity (see below) laws, giving direct redress through the courts and possibly criminal penalties for improper surveillance or sharing. The common law position, where one may use any name provided there is no fraud, may need to be updated and strengthened to permit anonymity and pseudonymity to survive.

Informational Privity

48. We suggest that there is a missing concept in relation to the sharing of information, and that it ought to be analogous to the grant of rights in forms of property, in that information is received from a particular source for a particular purpose, and it ought therefore to be the case that the use of personal information depends on a chain of title. A supplier ought not to be able to grant greater usage than he has himself has. Though potentially complicated in detail, this model offers a coherent way to place control of personal information ultimately where it belongs: in the hands of the subject.

Government sharing and matching subject to judicial control

49. Just like physical searches, we believe that data-sharing and data-matching or –mining exercises by government should be permitted only with good reason (such as reasonable suspicion of an offence) and subject to due authorisation depending on the reason. Matching and mining in particular are of the nature of

general search warrants and ought to be permitted only on judicial authority. Fishing expeditions, where there is no evidence of a crime or other pressing reason, ought to be barred.

Protection of common law standards

50. The common law doctrines of *ultra vires* and confidentiality have grown up precisely as protection for the individual against abuse of power. They should be guarded.

8 June 2007

References

[1] See discussion in Guy Herbert *The Biggest Christmas Tree* Garden Court News, Autumn 2005, where it is argued the Identity Cards Bill confers the power of civic life and death on the Home Secretary.

[2] See, Cabinet Office paper *Transformational Government—enabled by technology* Cm6683, November 2005 http://www.cio.gov.uk/transformational_government/strategy/

[3] DCA, September 2006 http://www.foi.gov.uk/sharing/information-sharing.pdf

[4] Eg Children Act 2004, s 12.

[5] Eg Serious Crime Bill, as brought from the Lords 2007, cl.66 which modifies the Data Protection Act 1998 to vitiate any relevant protection.

[6] See, for example, Bruce Schneier, *Secrets & Lies: digital security in a networked world*, Wiley, 2000.

[7] "Your honour, it's about those Facebook photos of you at 20"—The *Observer*, 20 May 2007. http://observer.guardian.co.uk/comment/story/0,,2083798,00.html

[8] Which is to say, they are assumed to consent if they fail to object, though this is now banned in relation to commercial data-sharing.

[9] The beginning of one might be found in the new "voyeurism" offence under the Sexual Offences Act 2003. The notional common law offence of eavesdropping is often referred to, but I have been unable to find a case in English law.

[10] Following the US Supreme Court in *Griswold v Connecticut*, 1965.

[11] "I see no reason why there should not be an obligation of confidence for the purpose of enabling someone to be the only source of publication if that is something worth paying for" Lord Hoffman in the Hello! case (http://www.publications.parliament.uk/pa/ld200607/ldjudgmt/jd070502/obg-5.htm at 120.)

[12] As for example intended by the Identity Cards Act 2006, see Regulatory Impact Assessment, November 2004 http://www.homeoffice.gov.uk/documents/ria-identity-cards-bill-251104?view=Binary or pursuant to Criminal Records Bureau disclosures.

[13] ID Cards—Benefits Overview, p12 http://www.identitycards.gov.uk/downloads/2005-06-27_Identity_Cards_Scheme_Benefits_Overview.pdf

[14] Simon A Cole *Suspect Identities* Harvard UP, 2001.

[15] As the Criminal Records Bureau enhanced disclosure procedures imply.

[16] Eg that described in the LSE Identity Project Report, June 2005 http://identityproject.lse.ac.uk/identityreport.pdf

[17] Which incidentally means they are likely to work better in practice.

Memorandum by Martin Twomey, Hackney and Shoreditch NO2ID Group

When a recent conversation turned to the creeping surveillance society and identity cards the person I was speaking to told me about his elderly parents' recollections of WWII identity cards. They spoke of the British public a few years after the war ended becoming fed up with growing intrusion and harassment, with every jobs-worth official from post office clerks to railway porters, bus inspectors to bobbies on the beat constantly demanding people's identity cards. They told of people gathering in the streets to burn their cards in defiance of what had come to symbolise an overbearing and ever more intrusive state.

And well they might! Wartime identity cards, when introduced in 1939, had just three administrative functions: national service, national security and food rationing. Within 11 years this had risen to 39, and showing your identity card for the most trivial of purposes had become routine.

This began to unravel on 26 June 1951, due to the defiance of one man: Clarence Willcock. Mr Willcock refused to produce his ID card when stopped by a police officer. Lord Goddard, Lord Chief Justice, summing up in the resulting appeal court case said; "To use Acts of Parliament, passed for particular purposes during war, in times when the war is past—tends to turn law-abiding subjects into lawbreakers, which is a most undesirable state of affairs". As a result, in 1952, as Winston Churchill abolished the last compulsory ID scheme in Britain.

Throughout the ID Card debate we have been repeatedly told the cards, and the vast database behind them, the National Identity Register, will help fight crime, identity theft, illegal immigration, benefit fraud, and terrorism. The detail of these claims has been analysed and discussed at length and is beyond the scope of this submission. But experts and officials in many fields have argued soundly that they are exaggerated, misleading or plain wrong. But the spinning of those lies persists, as though on the Goebbels principal that if you tell a lie big enough and keep repeating it, people will eventually come to believe it.

The success of these lies however would seem to be central to the aims of those pushing for the National Identity Register and a wider surveillance culture. A 2004 YouGov survey for Privacy International indicated: "millions of people would take to the streets or break the law to fight the UK Government's proposed national ID card" and "more than a million people would go to prison rather than register for a card".[1]

The tactic to disarm such popular opposition has been to generate a climate of fear about the issues mentioned above, and then proffer greater surveillance and ID cards as the solution.

Against this background of fear a sizeable part of the population seems to have lost or abandoned its capacity for critical thought. Last November the Information Commissioner Richard Thomas stated: "Two years ago I warned that we were in danger of sleepwalking into a surveillance society. Today I fear that we are in fact waking up to a surveillance society that is already all around us." But there is no outcry from this ever more scrutinised society—why? Two factors would seem to explain this: "stealth" and "mission creep". Essential tools for anyone wanting to subdue a population, they are shrewd alternatives to the jack-boot enforcement of other times and places, but crucially, they can achieve the same results. One could be forgiven for feeling that the secret would appear to be to progress slowly in small increments, introducing "necessary" and benign legislation, which once passed, provides powers that can be employed in ways which could not have been foreseen by the public, press, or Parliament whose job it should be to filter out such dangerous aims.[2]

This sounds like conspiracy theory of course. But take the Terrorism Act (section 44), it allows the police to detain without the need to demonstrate "reasonable suspicion". This happened in 2003 no less then 995 times against peace protesters. (Liberty report "Casualty of War" 2003).[3] The Act was even used to expel the now famous heckler from last year's Labour party conference. Under The Serious Organised Crime and Police Act, two people were convicted for "reading"—reading out the names of UK soldiers killed in Iraq at the Cenotaph. (Liberty press release—26 January 2006)[4] The Protection From Harassment Act, passed to protect women from stalkers was used to imprison a peaceful protester. (indymedia.org; Demonstrator sent To Lewes Prison—17 June 2005)[5] These are not isolated cases of abuse, the list goes on.

If one looks back to 1934 at the hidden agenda of surveillance built into the WWII ID cards, a far less intrusive device, one can see the dangers that exist today. Sylvanus Percival Vivian, Registrar-General responsible for designing the WWII ID card, identified a strategy referred to as "parasitic vitality": "if it cannot be given enough real peace value of its own it must be given a borrowed and artificial peace value . . . its use and production and the quoting or recording of the number upon it must be made obligatory in regard to as many as possible of the organised activities in close touch with the life of the people".[6] Investigation shows a similar philosophy behind the façade of the Identity Cards Act 2006. When one looks at this in the wider context of things like ePassports that log data about personal travel, centralised medical records without privacy, fingerprinting and biometrics in schools, the Children Act "Information Sharing Index", proposals for fingerprinting in pubs, police roadside fingerprinting, the recording of all car journeys as a matter of course using ANPR, the proposed addition of listening devices and facial recognition on public CCTV systems, it is impossible not to believe that a faction of the state has developed an unhealthy obsession with possessing all the information it is possible to possess on all of the population.

What is clear is that the ID card project alone, if implemented, will in time lead to a population totally dependant upon it for most of the normal transactions of their daily social and commercial existence. Another and even more pernicious aspect of the scheme's "collateral damage" will be its impact on minority groups. In 2003 criminologist Ben Bowling found that African-Caribbeans are 27 times more likely than Whites, and Asians 18 times more likely to be stopped under the Criminal Justice and Public Order Act.[7] The current DNA database holds samples on hundreds of thousands of innocent people, including 24,000 juveniles, who were never cautioned, charged or convicted of any crime. 38% of all black men are represented on that database, while just 10% of white men are.[8, 2] In other European countries with less intrusive identity systems we see shocking abuse of minorities: In France young people North African descent complained they were asked to produce their papers several times a week following new laws in the mid 1990s. In Belgium, a citizen who produced her ID card was disbelieved by police, who decided she must be an "illegal" carrying a fake document because she was of African origin. She was detained for three days and almost deported to a country she had never seen.[9]

But this Government deny legislation supporting a surveillance culture will be abused yet we witness a string of abuse of existing laws. They deny our civil liberties are being eroded while limiting our freedom to assemble and speak. In the same vein, they deny that identity cards will be detrimental to society, yet it is plain to all who examine the detail, that this Act of Parliament will alter forever the balance of power between the rulers and those ruled. It is ironic that such a seismic shift in this delicate balance, and in this direction, has not been seen in Western Europe since the 1930s.

But what has a Government of any colour to gain from such surveillance? The creeping surveillance and ID card project, once embedded in our culture, will by its insidious nature, create a widespread subconscious fear of "making trouble" of any kind. Those who are marginalized and most need a voice will be least able to speak out for fear of the ever-present threats, which such a system of total centralised surveillance and control embodies.

It must therefore be hoped that the current review will recognise the disastrous direction taken by recent legislation and thinking, and that a more enlightened group of people will take the state back from the brink of this Orwellian abyss, people who value fundamental freedoms, who understand and will defend the subtleties of the relationship between state and individual. In the words of Edmund Burke: "The price of liberty is eternal vigilance."

June 2007

Reference Notes

[1] Editor—PublicTechnology.net—2004. A public opinion survey commissioned by watchdog group Privacy International. http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=1083

[2] Henry Porter—Blair's Big Brother Legacy—June 30, 2006. http://www.craigmurray.co.uk/archives/2006/06/blairs_big_brot_1.html

[3] Liberty report *Casualty of War*—2003. http://www.liberty-human-rights.org.uk/issues/pdfs/casualty-of-war-final.pdf

[4] Liberty press release—26 January 2006. http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2006/first-case-under-new-protest-law.shtml

[5] indymedia.org—Anti-EDO demonstrator sent To Lewes Prison. 17 June 2005. http://lists.indymedia.org/pipermail/imc-uk-features/2005-June/0616-qz.html

[6] Jon Agar, Department of History and Philosophy of Science, University of Cambridge.—Identity cards in Britain: past experience and policy implications. November 2005. http://www.historyandpolicy.org/archive/policy-paper-33.html

[7, 8] Arun Kundnani—"Anti-terrorism" policing leads to arbitrary use of stop and search—Independent Race And Refugee News Network—20 January 2004.

[8, 9] Henry Porter—We don't live in a police state yet, but we're heading there—The *Observer*—22 January 2006

[9, 10] Arun Kundnani—ID cards: implications for Black, Minority Ethnic, migrant and refugee communities—The Institute of Race Relations 26 May 2005.

Memorandum by the Open Rights Group

1. Introduction

1.1 New technologies for data collection, data storage and data manipulation appear to offer governments the tantalising opportunity to find out more and more about those they govern. This opportunity has been seized many times over the last few years, in the name of efficiency, economy or security. The resulting armoury of legislation[42] and practice[43] is eye-watering; in effect it legitimises the mass surveillance of UK citizens. This consultation is therefore a timely one and we welcome the opportunity to respond.

2. The Impact of Surveillance

2.1 Pervasive surveillance degrades human dignity. The erosion of privacy—a fundamental human right—that such surveillance represents is neither proportionate to its stated aims nor wholly legitimate according to the purpose it serves.

2.2 When data gathering becomes routine and automatic, but when the protections afforded those data are uncertain and the purposes to which they might be put unclear, the relationship between citizen and state changes fundamentally. Citizens are no longer aware when their privacy is being breached, for what reason or purpose, and must therefore assume they are under a constant "watch".[44] This is highly likely to alter their behaviour over time.

2.3 For example, faced with this threat, those who engage in unpopular practices (activities often considered most protected: religious, sexual, political) effectively lose the right to hold their viewpoint or to act in a manner theoretically protected by law, because they cannot be sure their personal information will not be leaked by contractors or corrupt civil servants, or indeed simply published through incompetence.

2.4 Further, surveillance has the potential to undermine the work of communities, transferring the responsibility to "look out for each other" to a centralised, faceless, database state. This loss of local control in favour of central control leads to alienation and, in turn the demand for a more "disciplinary" society, led from the centre.

3. Constitutional Protections

3.1 In theory, the Data Protection Act, grounded in the right to privacy, should go some way towards protecting UK society from these outcomes. But in practice, its enforcement record is weak and there are currently no effective criminal sanctions for its breach.

3.2 When banks dump personal data in outdoor rubbish bins, in direct contravention of the Act, their punishment is to sign a form saying they won't do it again.[45] When the identities of staff at Network Rail and the Department of Work and Pensions are stolen from a compromised HMRC portal to defraud the tax credit scheme, HMRC escapes unpunished.[46, 47]

---

[42] Some recent surveillance state Acts and bills:
- Immigration, Asylum and Nationality Act 2006 http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321295
- Terrorism Act 2006 http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321013
- Identity Cards Act 2006 http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321581
- UK Borders Bill 2007 http://www.publications.parliament.uk/pa/pabills/200607/uk_borders.htm
- Serious Crime Bill 2007 http://www.publications.parliament.uk/pa/pabills/200607/serious_crime.htm
- Digital Switchover (Disclosure of Information) Bill 2007 http://www.publications.parliament.uk/pa/pabills/200607/ digital_ switchover.htm
- Statistics and Registration Service Bill 2007 http://www.publications.parliament.uk/pa/pabills/200607/statistics_and_registration_ service.htm

[43] Public and private practices include:
- RFID-based tracking systems in Passports and Oyster cards;
- The monitoring of internet use through search engine and ISP logs;
- Police National DNA database;
- Fingerprinting practices in crime preventaion and school identification systems;
- CCTV;
- Number-plate recognition systems (National Vehicle Tracking System, London Congestion Charge);
- Facial recognition cameras;
- NHS Care Records Service;
- The Children's Index; and
- NpfIT (NHS data spine);

[44] See McCullagh, Karen (April 2005) "Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance", 20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: the New Digital Legal World?

[45] Press Association, 13 March 2007 "Banks 'dumped personal information in bins'", http://money.guardian.co.uk/saving/banks/story/0,,2032962,00.html

[46] The Register, 18 January 2006, "HMRC tax debacle spreads", http://www.theregister.co.uk/2006/01/18/hmrc_tax_debacle/

[47] An register of "UK Privacy Debacles" is maintained by the Open Rights Group community at http://www.openrightsgroup.org/orgwiki/index.php/UK_Privacy_Debacles

3.3 Indeed, it may be true that constitutionally, the UK is protected from the threats of a surveillance state. But unless these protections are enforced, they are meaningless.

4. About the Open Rights Group

4.1 The Open Rights Group is a grassroots digital rights advocacy group based in the UK. It aims to increase awareness of digital rights issues, help foster grassroots activity and preserve civil liberties in the digital age. It is funded by individual donations and small grants.

June 2007

Memorandum by The Royal Academy of Engineering

1. *How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and state in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

1.1 As the capacity to store and search data held electronically continues to grow, so more and more personal data is collected and retained. The balance between citizen and State is affected when that data is collected without citizens' consent or knowledge, when they have no choice to "opt out" of surveillance, and when data collected for a specific purpose is used in ways the citizen did not foresee.

1.2 The rise of camera surveillance probably has the greatest impact as individuals in public spaces cannot refuse consent for the recording of their image. Often people do not know that a particular area will be under the view of surveillance cameras and they may not be aware of when they are being filmed. The increase in such surveillance means that the 'big brother' State becomes more than just a cliché. Authorities are watching citizens for increasing proportions of their daily lives and citizens have no power to reject such surveillance.

1.3 This imbalance of power between the citizen and the state can be addressed by introducing an element of "reciprocity" into the surveillance relationship. Reciprocity could be achieved by allowing the public access to detailed information about the siting of cameras. For example, a website could be launched containing maps which indicate the locations of cameras, and sample images from cameras demonstrating their range. This would allow individuals and communities to raise complaints should they feel that particular cameras are unnecessary or excessively intrusive.

1.4 In the private sector, schemes like the Oyster travel card introduced by Transport for London and store loyalty cards involve collection of data about individuals. Although these are voluntary, people would miss out significantly on benefits and convenience if they refuse them or use them anonymously. These technologies and services effectively collect data about peoples' journeys and purchases by stealth, as the user may be unaware that such information is generated when they are used. It is not obvious that a loyalty card designed to attract customers into a store will be used to harvest personal information used in marketing, and it is not clear that the card should have to function in that way.

1.5 People should be able to choose not to give away personal information in the process of "registering" a loyalty or travel card. This is similar to the choice not to receive further marketing information when signing up for a service. Although there may be some disadvantages in holding a travel or loyalty card anonymously (eg, losing the possibility of retrieving credit on a lost card), the individuals who hold them should be able to choose to take that risk.

1.6 Risks arise when data collect by the private sector is used by the public sector—eg, the police accessing footage from a store's CCTV or examining Oyster card or store card records. The potential merging of private and public data sets—where the former are collected with consent for a specific purpose—should be carefully monitored.

2. *What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might that line be identified?*

2.1 Surveillance and data collection is constitutionally proper when it is done in the interests of the citizen. For example, the collection, retention and sharing (between appropriate parties) of data about individuals' health is essential for providing proper health care. Notwithstanding the notable difficulties encountered in the NHS's move to electronic patient records, it is right and proper that the health service update the means by which it collects, stores and shares patient information in order to improve the service that the patient receives.

2.2 Similarly, the use of camera surveillance in areas of high crime can be justified if it aids in the conviction of criminals. Thus it can support the police service in fulfilling their duty to protect the public.

2.3 In such cases there is a clear benefit from surveillance and data collection or processing. However, as these benefits diminish they are outweighed by factors of constitutional propriety. Camera surveillance is less beneficial in areas where there is less crime. Although it might seem obvious that increased surveillance prevents crime, evidence for this is low (see Home Office Research Study 292, *Assessing the Impact of CCTV*, by Martin Gill and Angela Spriggs). When blanket surveillance is employed, its benefits are outweighed by the fact that innocent citizens are being watched and are thus experiencing diminished privacy. In such circumstances concerns about constitutional propriety outweigh any claimed benefits.

2.4 In short, surveillance and data collection are acceptable if they bring a clear benefit to members of the public. Collecting data or filming on streets on the basis of the mere "chance" it will be useful is neither constitutionally proper nor an efficient use of resources. (This point is especially relevant to the National DNA Database, discussed under point 6 below.)

2.5 This is not to say that there is a clear line between effective and beneficial surveillance and "constitutionally improper" surveillance. The Royal Academy of Engineering's report on this subject was entitled *Dilemmas of Privacy and Surveillance* because the choice between privacy and increased security or convenience often poses a dilemma. In most cases there is a delicate balance to be struck. Therefore, any proposed surveillance system, or any service which involves the collection and processing of personal data, should only be introduced with a clear justification of how its benefits outweigh any limitation it may pose on individuals' privacy.

3. *What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

3.1 The UK is a signatory to the UN Declaration of Human Rights and has incorporated the European Convention of Human Rights in UK law. Both of these stipulate that an individual has the right to freedom from interference in their private life, home and correspondence.

3.2 Collecting and retaining information about peoples' everyday movements and activities, when those activities are perfectly law-abiding, should be considered an infringement on a person's right to privacy. Whether this information is collected by cameras, via the ticketing systems on public transport, or in the course of purchasing everyday goods, a person's right to privacy is infringed unless they have explicitly consented to the collection of data or there is a strong justification in terms of peoples' wellbeing or safety.

4. *What impact do surveillance and data collection have on the character of citizenship in the 21st century, in terms of relations with the State?*

4.1 Increased camera surveillance is employed in order to deter and catch criminals; greater sharing and centralisation of personal information is used to identify fraudsters in the public or private sector. Thus the innocent majority are subject to the same measures as the criminal minority and are treated as potential criminals. The State in effect treats citizens as posing an inherent risk which must be controlled. This shows a lack of trust on behalf on the State in its citizens and is likely to cultivate a reciprocal lack of trust.

4.2 People from minority groups, particularly young black males, are more likely to be the subjects of surveillance. For example, they make up a disproportionate number of the entries on the National DNA Database. There is a danger of such social groups becoming increasingly marginalised, resulting in a breakdown of mutual trust between different minority groups and between those groups and the State.

5. *To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?*

5.1 The Data Protection Act 1998 (DPA) can only safeguard constitutional rights if the Information Commissioner has sufficient power to successfully prevent or punish breaches of the act. Recently it has become possible for custodial sentences to be passed for serious breaches of the DPA—this is a welcome development as it increases the strength of the DPA as a deterrent.

5.2 However, the Information Commissioner can only take action against an organisation if there has been a complaint made against it. It is not possible for the Information Commissioner's Office (ICO) to perform "spot checks" or audits such as are possible with, for example, environmental health regulations. Without such powers to ensure that individuals and organisations are adhering to the principles in the DPA then the DPA

cannot effectively safeguard constitutional rights. In addition, greater clarity over the information that an organisation holds about individuals will make it easier for an individual to check that information and raise a complaint with the ICO if necessary.

6. *Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

6.1 The DPA makes special concessions for the use of data in the investigation of crimes. However, it is important that the collection and use of personal data for criminal investigations is regulated.

6.2 The National DNA Database is an ever-growing repository of DNA profiles and samples collected from suspects, witnesses and volunteers. The existence and use of this database raises significant questions regarding the rights of those individuals on it. Once a profile is added to the database it is retained, even if collected from a witness, a volunteer, or a suspect who is cleared of involvement in a crime. These are kept on the basis of the mere chance that they will be useful in future investigations—surely something that the DPA would rule out. DNA profiles can be used to identify family relationships or to predict susceptibility to disease. They therefore constitute sensitive personal information that an individual should have the right to withhold if there is no specific need for it in the investigation or prevention of crime.

6.3 Since the use of personal information in criminal investigations is a quite specific issue, there is an argument for new legislation and the establishment of a new body to oversee the collection, retention and use of bioinformation (including DNA profiles, fingerprints, facial images and so on). This body should have powers to check that records are not kept for excessive periods or without clear justification. Alternatively, the role of the Surveillance Commissioner could be extended to cover the collection, retention and use of bioinformation by the police service.

6 June 2007

Memorandum by Runnymede Borough Council

1. This evidence is based on 10 years experience of managing a public space CCTV system which in that time has grown from 40 cameras to over 300. The system is operated by Runnymede Borough Council for the benefit of local people.

2. The system was introduced by The Council in response to demands from constituents made to members as they went about their ward business. I was recruited as operational manager with a background of 32 years in Surrey Police including Divisional Command at Woking.

3.. As a basic policy it was decided to be overt with well signed and very obvious. cameras. It is obvious in which direction the cameras are pointing.

4. Carefully managed visits of residents groups and others have taken place throughout the life of the control centre in a spirit of openness but with a care for data protection issues. About 2,000 individuals have visited the centre and only a handful has ever raised a liberty or privacy issue.

5. Visitors have been asked if they have such concerns and have always said no, or, not when it is managed properly. The most frequent comment is that if you have done nothing wrong you have nothing to hide. The other common comment is that they are in a public place so can be expected to be seen by others anyway.

6. Visitors have also frequently commented that they feel safer and it increases their liberty to enjoy the areas covered by CCTV. This feeling is supported by independent survey which revealed that the fear of crime affecting a person's lifestyle has fallen from 41% in 1996 to 22% in 2004, the latest survey.

7. The control centre has always attempted to maintain the highest standards regarding the staff which are directly employed, the equipment designed to provide evidential quality pictures, and the management practices and procedures which comply with all legislation and guidance on best practice.

8. It is misleading to think of it as a "security camera" system which is far to narrow to encompass what the system can and does achieve. Whilst standards are essential there are therefore dangers if only security industry standards are applied.

9. The control centre deals with a full range of caring tasks for the local community including:

(i) Public Space CCTV Monitoring;

(ii) Careline call handling;

(iii) incident management;

(iv) out of hours service calls;

(v) lone worker support service

(vi) calls from public help points;

(vii) access controls to sheltered homes; and

(viii) access controls to public open spaces.

10. The control centre is a centre for local security and incident management and works closely with the following partners:

(i) Ashford & St Peter's Hospitals Trust;

(ii) BMC Software;

(iii) Hillswood Business Park;

(iv) Royal Holloway, University of London;

(v) South West Trains;

(vi) Spelthorne Borough Council;

(vii) Surrey County Council; and

(viii) Thorpe Park.

11. Working together in this way enables a more effective management of incidents which can vary from minor crime or nuisance, to major incidents of flooding. It also provides an opportunity to influence the standards of CCTV installations and management by other organisations in the area.

June 2007

Memorandum by Dr T Thomas, Reader in Criminal Justice Studies, School of Social Sciences, Leeds Metropolitan University, Leeds

Abstract

This submission explores the extent to which non-police agencies have access to the Police National Computer (PNC). These include other law enforcement agencies and some private sector agencies. The information held on the PNC has normally been considered confidential and for police purposes only. The extent of the current access is not widely known and has seemingly taken place without democratic oversight or debate.

The Police National Computer (PNC)

1. The Police National Computer (PNC) came on line in 1974 and since then has been regularly refurbished and kept up to date. It holds information essential to police work, including criminal records, details of stolen vehicles, wanted or missing persons. Offenders who have given DNA samples etc. This information has always been treated as highly confidential and sanctions apply to officers who release information improperly.

2. As the PNC has developed and grown in stature its customers have also grown. In 1992 Parliament was told that only the DVLA and HM Customs and Excise had direct access to the PNC for "read-only" purposes, although plans to improve the speed of communications between the PNC and individual forces "could be extended later to other agencies in the criminal justice system" (*Hansard* HC Debates, 3 February 1992, cols 109–110). Today this position has changed. Apart from servicing the needs of the 43 police forces in England and Wales, the eight forces of Scotland and the Northern Ireland Police Service, other smaller police forces and specialist units have direct access to the PNC as do a number of non-police agencies—some of them beyond the criminal justice system—who have demonstrated a need for access.

3. A list of some of these other forces, specialist units and non-police agencies has been compiled in Table A. This is not presented as a definitive list but as examples of how wide the dissemination of information on the PNC has reached. Access is agreed by an ACPO (Association of Chief Police Officers) "PNC Access Application Panel" and "PNC Data Access Agreements" duly drawn up; those with direct access must comply with the ACPO Information Systems "Community Security Policy".

4. Most of these recipients of PNC-held data have "read only" access and no facility to update. Some only have access to one database such as the DVLA with its access to vehicle information and some only have access to names of people with a criminal record rather than the full record from Phoenix (as explained at *Hansard* HC Debates 18 April 1995, Col 87–8).

5. A customs officer, for example, has described how they use the PNC:

> . . . we're able to use the PNC to gain background information . . . what we want to know is if someone we suspect—say of drugs smuggling—has a criminal record or if a vehicle has any markers against it. So we have limited access to the PNC databases for vehicles and names.
>
> ("PNC keeps Customs and Excise in the picture", *PITO News*, Issue No 14, December 1998).

6. A total of 1,638 Customs Officers out of 25,000 reportedly had access across the UK (*ibid*).

7. In prisons access has proved particularly useful with the assessment and categorisation of newly arrived prisoners; 38 prisons had access by 1999 (Prison Service Order 1999, No 0905).

8. The spreading use of the PNC has been facilitated by the PITO (Police Information Technology Organisation) Directorate in charge of the computer. The "Phoenix Links" project sought out new customers after 2001 and this later became known as the PNC Application Integration Infrastructure. According to PITO's Director of Operational Services at the time:

> . . . we saw the need some years ago to develop a new approach for the implementation of system-to-system links between PNC and the increasing number of applications that were beginning to arise on third party systems. (quoted in "Jurors technology breaks new ground", *PITO News* Issue 30, 2002).

9. Exactly how many agencies have a direct link is uncertain as no definitive list appears to exist. A four page document describing non-police users of the PNC as at 29 April 2002 was produced at an Information Tribunal hearing in 2005, but this document has not been made public. The list was shown to David Smith, the Assistant Information Commissioner during the hearing:

> . . . it is fair to say that Mr Smith expressed some surprise . . at the length of the listed organisations (and) . . . he asked the not unnatural question "is it really necessary for all these organisations individually to have access?"
>
> (The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner, Information Tribunal 2005 at para 126).

10. When asked in Parliament how many individuals (as opposed to agencies) have access to the PNC, Home Office Ministers always say the information is not available (see eg *Hansard* HC Debates 22 January 2004, col 1440W and 9 February 2006, Col 1436–7W).

11. Apart from exact numbers and lists of those with access the spreading use of the PNC could be feeding a culture that says this information is not that confidential after all. Informal access may be growing alongside the formal. Co-operation between the police and housing departments, for example, has been encouraged to tackle crime and anti-social behaviour. In Nottingham a housing official has explained how they get information from the PNC, working from the same premises as the police:

> . . . we actually had a PNC terminal here, so I could literally go to the sergeant and say "have you got anything on this individual?" and within a matter of minutes . . . he could give me information on that individual. (cited in Burney, 2005: 126)

12. Housing departments have no direct access to the PNC but working together and sharing information has made access fairly easy. The use of vehicle-based terminals and hand-held terminals arguably makes the "policing" of confidentiality even more difficult.

Table A

AGENCIES HAVING DIRECT ACCESS TO THE POLICE NATIONAL COMPUTER

British Transport Police;

Civil Nuclear Constabulary (previously the UK Atomic Energy Authority Constabulary);

Isle of Man Police;

States of Jersey Police;

Guernsey Police;

Ministry of Defence Police;

Royal Military Police;

RAF Police;

Secret Intelligence Service;

Security Service;

National Ports Office;

National Identification Service;

National Criminal Intelligence Service;

National Crime Squad;

Scottish Crime Squad;

Scottish Criminal Record Office;

Northern Ireland Criminal Record Office;

Regional Criminal Intelligence Offices;

Port of Dover Police;

Hendon Data Centre;

Police Staff College, Bramshill;

Police Information Communication Technology Training Services (PICTTS), Leicester;

Immigration Service;

HM Revenue and Customs;

Post Office;

Financial Services Authority;*

National Health Service;*

Department of Trade and Industry;*

Office of Fair Trading;*

Central Summoning Bureau (Dept of Constitutional Affairs);

Department of Work and Pensions* (previously Dept of Social Security);

Criminal Records Bureau;

Forensic Science Service;

Motor Insurance Database;

HM Prisons (some of them);

National Enforcement Service;

Drivers Vehicle and Licensing Authority; and

Schengen Information System.

* for prosecution purposes only.

Sources: Hansard HC Debates 22 March 1995 col 200; 18 April 1995 cols 87–8; 26 April 1995, cols 566–7; 5 February 2002, col 858w; 8 July 2003, col 716w; 15 July 2003, col 278w; 4 July 2005, col WA63.

PITO News Issue No 8 (pp 14–15); No 9 (p 3); No 29 (p 11); No 30 (pp 8–9); No 35 (pp 8–9). Home Office (2003(a)) Annex B Group 4.

13. In April 2006 the Government announced its intention to replace the PNC as such by a new Police National Database costing £367 million and due for implementation by 2010. While this new Database was under development funding would be made available "to update the hardware platform of the PNC (to) ensure it remains fit for purpose until the Police National Database is fully in service" (*Hansard* HC Debates 19 April 2006, Cols 18WS to 19WS).

May 2007

Memorandum by Hugh Tomlinson QC

1. *Are there any existing constitutional conventions or principles that are threatened by the spread of surveillance and data collection?*

The common law protection of privacy was focussed on the protection of the integrity of the home. The fundamental human right to protection against unlawful searches and seizures is part of the English common law and passed into the Fourth Amended to the United States Constitution (see *A–G of Jamaica v Williams* [1998] AC 351, 358). This was, in turn, the source of Article 8 of the ECHR. I do not think that there are any

specific constitutional conventions or principles directly relating to surveillance or data protection. The absence of any general right of "privacy" in English private law is very well known and the domestic courts refused to develop the law to cover telephone tapping in the well known *Malone* case.[48]

Are there principled limits that we might want to impose on the surveillance and data collection powers of the state?

I do not think that "absolute" limits could be imposed as the state requires surveillance and data protection powers for a very wide range of legitimate purposes which cannot sensibly be delineated in advance. A strong requirement could, however, be placed on the State to provide clear and specific justification for surveillance and data collection, allied to clear rights of access to information which is held and strong enforcement powers.

2. *What do you regard as the major legal obstacles to the better protection of privacy in the United Kingdom?*

The major legal obstacle to the better protection of privacy in the United Kingdom is the absence of a strong "constitutional" privacy right. Although the Courts have, in response to the impetus provided by the Human Rights Act 1998 developed a wide range of "constitutional common law rights" in other areas, privacy has not been so recognised and Article 8 has, at present, only partially filled the gap. The absence of such a right means that invasions of privacy do not require "strong justification" or, put another way, are not subject to the kind of "strict scrutiny" applied when, for example, there is an interference with the right to liberty.

At present English domestic privacy law only provides limited protection in area of intrusive surveillance—the first "aspect" of the tort of privacy in the United States.[49] The law in this area remains unclear although the United Kingdom does have a "positive obligation" under Article 8 of the ECHR to protect citizens from such intrusion and is, therefore, required to have appropriate domestic laws in place.

To what extent are these problems likely to be resolved by the courts in the coming years?

It seems likely that the Courts will continue to develop domestic privacy law but will, nevertheless, remain cautious in reviewing the surveillance and data collection powers of the State. In my view, the Courts are likely to regard any major change in this area as a matter for Parliament.

Do you think that Parliament needs to take a more proactive legislative role in relation to surveillance and data protection issues?

I do think that Parliament needs to legislate in this area.

3. *Do you think that Article 8 of the European Convention on Human Rights (ECHR) provides a good basis for the protection of privacy rights in the United Kingdom?*

As already mentioned, Article 8 is the ECHR version of the Fourth Amendment and the common law protection against "warrantless searches". Although it has been greatly expanded in scope by the European Court of Human Rights ("ECtHR") over recent decades, it is not directly focused on the surveillance and data collection issues and, as a result of the caution of the ECHR (and following it, the domestic courts) does not provide "strong protection" against State surveillance.

Do you think that the scope of Article 8(2) is too broad? Do you think the grounds on which it is justifiable to interfere with the right to privacy should be restricted?

I do not think that this question is correctly formulated. In order to justify an interference with Article 8 rights, it must be shown that the state is acting lawfully, for a legitimate aim and that the interference is "necessary in a democratic society", that is, proportionate to the legitimate aim. The crucial question is always that of proportionality. Neither the ECHR nor the English courts have applied a rigorous proportionality test to the justification of interferences with Article 8. If the grounds on which it was justifiable to interfere with the right to privacy were to be restricted this should be done by requiring a stricter proportionality test to be satisfied.

[48] *Malone v Commissioner of Police (No. 2)* ([1979] Ch 344); Mr Malone's application to Strasbourg was successful (*Malone v United Kingdom* (1984) 7 EHRR 14) which, in turn, led to the enactment of the Interception of Communications Act 1985.

[49] As summarised in the *Restatement of Torts*, 2nd Edn, para 625A.

Do you think that the right to privacy granted by Article 8 should be extended to public places? Could Article 8 provide an adequate basis for the better regulation of public area CCTV cameras?

The right to privacy under Article 8 arguably extends to public places already. This extension is supported by a number of ECtHR[50] and domestic decisions.[51] The case law is, however, not wholly consistent and, at present, Article 8 provides only a limited basis for regulation of surveillance.[52] If the applicant is successful in the case of *Marper v United Kingdom*[53] then the protection may be increased.

4. *Does the existing law of breach of confidence compensate for the deficiencies of Article 8? Is privacy better protected through the tort of breach of confidence?*

Although the domestic legal position is not wholly clear cut—the law being in a state of flux and development—it can properly be said that there is now a "tort" of misuse of privacy information. This is not a substitute for Article 8 but an "absorption" of Article 8 into the claim for breach of confidence.

"Misuse of private information" is, in substance, only relevant to the actions of private bodies as a direct "violation of Article 8" claim can now be made against public authorities under section 6 of the Human Rights Act 1998.

Do you think the development of a separate tort of privacy would help to protect the privacy interests of individuals and organisations?

The continuing development of a tort of privacy does help to protect privacy interests of individuals and organisations in relation to the actions of private bodies. I do not think that it has had a substantial impact on the protection of privacy interests vis-à-vis the State.

5. *How, if at all, have recent concerns about terrorism and security affected the development of privacy law in the UK? Has there been a retreat from a commitment to privacy in the wake of the events of 9/11 and 7/7?*

Recent concerns about terrorism and security have affected the development of privacy law in the UK in that surveillance and data collection have been easier to justify in the light of what are seen as the imperative requirements of counter-terrorism.

6. *Do you think the surveillance powers currently granted to the state are too broad? Does the existing regulatory regime—created by legislation such as the Data Protection Act and RIPA—provide adequate safeguards and restrictions?*

I do think that the surveillance powers currently granted to the state are too broad. They are subject to very light regulation—with intrusive measures easy to justify, not in general requiring independent judicial authorisation, and subject to little or no independent scrutiny.

Do you think that the exceptions and exemptions created under the Data Protection Act 1998 are too broad? How could they be narrowed?

I do not think that the exceptions and exemptions under the Data Protection Act 1998 are of themselves too broad. The regime under the Act is too complex and persistently misunderstood. Its revision would require action at the EU level.

[50] For example, *Peck v United Kingdom* (2003) 36 EHRR 41 and *Von Hannover v Germany* (2005) 40 EHRR 1.
[51] For example, *Campbell v MGN* [2004] 2 AC 457 and *Murray v Big Pictures* [2008] EMLR 12.
[52] see, for example, the recent case of *Wood v Commissioner of Police* [2008] EWHC 1105 (Admin) The taking and the retention of photographs by police officers of a person connected with a group opposed to the arms industry as he left a shareholders' meeting of the company that organised trade fairs for the arms industry did not amount to an unjustified interference with that person's right to respect for privacy under Art 8).
[53] The DNA database case in which judgment is awaited from the ECtHR.

Are the surveillance powers of the police and the security services adequately regulated? Does the law provide appropriate redress where those powers have been exceeded?

I do not think that the surveillance powers of the police and the security services are adequately regulated. The law plainly does not provide appropriate redress where powers have been exceeded—it being almost always impossible to determine whether or not this has taken place. In my view, the minimum safeguards should be:

(1) Independent judicial authorisation of all surveillance and other intrusive measures, such authorisation only to be given in accordance with strict statutory pre-conditions.

(2) A requirement that a full record be kept of the material put before the court in support of each application and the reasons why it was granted to enable the grounds for the application to be properly scrutinised after the event.

(3) A requirement that the subject of surveillance be informed that surveillance has taken place after the completion of the investigation.

(4) A mechanism for a full "merits review" of the lawfulness of surveillance with compensation payable to those who have been the subject of unlawful surveillance.

11 July 2008

Memorandum by G M Walkley

I would like to open my evidence with an indication of the ways in which the relationship between those in authority and the general public have altered in recent years. It was an accepted principle that the members of parliament and councils, in this country, were elected to serve the people and not to be the masters thereof. That our Civil Liberties along with our Human Rights and the Presumption of Innocence were paramount. All the principles upon which our Nation was built are being eroded by ever increasing intrusion by surveillance and data collection.

1. One has only to look at the enormous amount of data and surveillance that currently takes place or is proposed to see a marked change in the balance between the citizen and the state.

1.1. In the field of Education we have to supply data on pupils for E-Profiles, National Register of Gifted & Talented Learners and the National Pupil Database. Fingerprinting of students is accepted in a number of schools.

1.2. Home Office Initiatives on Young People include collecting data via Connexions, On Track and Positive Futures. Youth Inclusion Programme Management Information System hold data about children involved in YIPs and Junior YIPs. Reducing Youth Offending Generic National Solution is being positioned as having wider use in the "Every Child Matters" agenda. (RYOGENS system can record children of any age with the youngest known being just nine months.)

1.3. It seems to have become accepted practice that any young person can be approached for consent on data collection and sharing providing they considered by the agency to be "Gillick Competent".

1.4. The police are allowed to take DNA samples, and hold that person's profile on the Police National Computer, regardless of whether they are charged or cautioned. At the last count some 1.1 million innocent individuals, out of a total of over three million profiles were held on NDNAD. Familial searching is now routinely used to identify potential relatives of the person who left a crime scene sample.

1.5. The Government proposes to collect all the nation's medical records onto a central NHS database. This proposal is to be carried out without obtaining the consent of the individual patient, which both the BMA and the majority of GP's oppose.

1.6. The National Identity Register currently being introduced together with ID cards passed through Parliament on the basis that it would be voluntary, however being linked to the issue of a passport it is only voluntary if I elect not to travel abroad.

This is by no means an exhaustive list of measures which effect the daily life of all citizens, merely an indication of how the balance has changed. We are now in a society which is monitored from the cradle to the grave. Certainly it is my opinion that all those forms of surveillance that have been listed together with the vast numbers of CCTV cameras have the greatest impact on the balance between the State and citizens.

2. To my mind there are few forms of surveillance and data collection that can be considered as proper. However I would support measures to protect abuse of children, DNA profiling of convicted criminals and the use of familial searching in serious criminal investigations, eg cases of murder and rape. However when this familial searching is proposed application to the judiciary should be made or legislation enacted to detail under what circumstances this may take place. The executive claim that administrative, security or service

benefits of such activities are necessary cannot outweigh concerns about constitutional propriety and whether they are proportionate.

3. The collection of data and the surveillance carried out by public and private bodies transgress a citizens civil liberties and their right to privacy. As I stated in my opening remarks this is a matter of principle. The principle is that you are a sovereign citizen and you do not live by "government permission". A government is (or should be) the servant of the people, not its master. Privacy and freedom are yours by right and we only give governments permission to curtail these freedoms in very limited and important circumstances. It is not a proper function of government to engage in blanket surveillance of law-abiding citizens; or to instigate systems of compulsory identification; or to open a file on each citizen; or to criminalise citizens who refuse to comply.

4. The impact of surveillance and data collection has I believe a considerable negative effect on the general public with an increase in the mistrust of those in government together with alarm over how all this information will be used. We are continually hearing of cases where the security of these activities are breached. Only recently a new system for Junior Doctors, since abandoned, was hacked into and personal details revealed. Another example is the sale of used personal computers by Southend Council, which did not have the hard drive wiped by their agents, and details of a thousand children at risk became public. Certain details of the rich and famous will not be recorded on the National Pupil Register, with the Secretary of State, Rt Hon Beverley Hughes MP, maintaining "These decisions will be based on the level of the threat posed if their information becomes more widely available". This is the strongest indicator yet that the Government have no faith in the security of the systems.

5. Should the recent debate in the House of Commons over the effect of the Freedom of Information Act on MPs be a guide, the Data Protection Act 1998 offers little protection in safeguarding constitutional rights. Individuals have a wide range of rights under the Data Protection Act, including access, compensation and the prevention of processing, however these rights are limited. In addition to the many areas that are exempt, there are also special exemptions that apply to personal information relating to health, education and social services. The report by the Information Commissioner was succinct in stating that "the main problem is that the regulation of surveillance, including privacy and data protection, has not kept pace with the advance of surveillance technologies, practices and purposes".

6. There is a great need for additional constitutional protection for rights and privacy of the citizens of our country. I do believe that a fundamental change is required over the need to collect the personal data and the use of surveillance. At this juncture the perception is that all the measures are designed to control the citizens and are not of any benefit to the well-being of the nation. More stringent questions have to be asked as to the nature and purpose of these intrusions in our lives, are they relevant or not. The only protection that one can have in these circumstances is to stop further advances in the areas of surveillance and data collection and indeed roll them back.

In conclusion much of the data collection and surveillance that is currently carried out causes me great concern as does the prospect of the increase in this area in the coming months and years. I have to ask why this is being collected, what benefits do we enjoy from this, how will the information be used, what safeguards are in place to protect my privacy, are my human rights compromised? It may well be that these processes are benign at this time, however will this change in the future? I can find no reason to commend these information systems and on the contrary am alarmed at the ease with which security is breached. There is a very real need to have a citizens right to privacy, civil liberties and human rights protected in the most effective manner, be that enshrined in law or in a written constitution.

7 June 2007

Printed in the United Kingdom by The Stationery Office Limited
2/2009 404509 19585