House of Commons
Home Affairs Committee

A Surveillance Society?

Fifth Report of Session 2007–08

Volume II

Oral and written evidence

Ordered by The House of Commons
to be printed 20 May 2008

HC 58-II
[Incorporating HC 508-i–iv, Session 2006–07]
Published on 8 June 2008
by authority of the House of Commons
London: The Stationery Office Limited
£24.50

The Home Affairs Committee

The Home Affairs Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Home Office and its associated public bodies.

Current membership

Rt Hon Keith Vaz MP (*Labour, Leicester East*) (Chairman)
Tom Brake MP (*Liberal Democrat, Charshalton and Wallington*)
Ms Karen Buck MP (*Labour, Regent's Park and Kensington North*)
Mr James Clappison MP (*Conservative, Hertsmere*)
Mrs Ann Cryer MP (*Labour, Keighley*)
David TC Davies MP (*Conservative, Monmouth*)
Mrs Janet Dean MP (*Labour, Burton*)
Patrick Mercer MP (*Conservative, Newark*)
Margaret Moran MP (*Labour, Luton South*)
Gwyn Prosser MP (*Labour, Dover*)
Bob Russell MP (*Liberal Democrat, Colchester*)
Martin Salter MP (*Labour, Reading West*)
Mr Gary Streeter MP (*Conservative, South West Devon*)
Mr David Winnick MP (*Labour, Walsall North*)

The following Members were also members of the Committee during the inquiry:

Rt Hon John Denham MP (*Labour, Southampton Itchen)*
Mr Jeremy Browne MP (*Liberal Democrat, Taunton*)
Mr Richard Benyon MP (*Conservative, Newbury*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/homeaffairscom. A list of Reports of the Committee since Session 2005–06 is at the back of this volume.

Committee staff

The current staff of the Committee are Elizabeth Flood (Clerk), Jenny McCullough (Second Clerk), Elisabeth Bates (Committee Specialist), Sarah Harrison (Committee Specialist), Mr Tony Catinella (Committee Assistant), Mr Ameet Chudasama (Chief Office Clerk), Sheryl Dinsdale (Secretary) and Ms Jessica Bridges-Palmer (Select Committee Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Home Affairs Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 3276; the Committee's email address is homeaffcom@parliament.uk.

Witnesses

Tuesday 18 March 2008

List of written evidence

List of unprinted evidence

The following memoranda have been reported to the House, but to save printing costs they have not been printed and copies have been placed in the House of Commons Library, where they may be inspected by Members. Other copies are in the Parliamentary Archives, and are available to the public for inspection. Requests for inspection should be addressed to The Parliamentary Archives, Houses of Parliament, London SW1A 0PW (tel. 020 7219 3074). Opening hours are from 9.30 am to 5.00 pm on Mondays to Fridays.

Michael Nettleton

Christine Bloomfield

David Moss

Autism Rights

David Muxworthy

Nuffield Council on Bioethics

Angela Pinter

Jade Smith

Dr Mark Viney

List of Reports from the Committee during the current Parliament

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2007–08

First Report	The Government's Counter-Terrorism Proposals	HC 43
Second Report	Bulgarian and Romanian Accession to the EU: Twelve months on	HC 59
Third Report	Security Industry Authority	HC 144
Fourth Report	Work of the Committee in 2007	HC 226

Session 2006–07

First Report	Work of the Committee in 2005–06	HC 296
Second Report	Young Black People and the Criminal Justice System	HC 181 (*Cm 7217*)
Third Report	Justice and Home Affairs Issues at European Union Level	HC 76 (*HC 1021*)
Fourth Report	Police Funding	HC 553 (*HC 1092*)

Session 2005–06

First Report	Draft Corporate Manslaughter Bill (First Joint Report with Work and Pensions Committee)	HC 540 (*Cm 6755*)
Second Report	Draft Sentencing Guideline: Robbery	HC 947
Third Report	Draft Sentencing Guidelines—*Overarching Principles: Domestic Violence* and *Breach of a Protective Order*	HC 1231
Fourth Report	Terrorism Detention Powers	HC 910 (*Cm 6906*(
Fifth Report	Immigration Control	HC 947 (*Cm 6910*(
Sixth Report	Draft Sentencing Guideline: Sexual Offences Act 2003	HC 1582

Oral evidence

Taken before the Home Affairs Committee

on Tuesday 1 May 2007

Members present

Mr John Denham, in the Chair

Ms Karen Buck	Gwyn Prosser
Mr James Clappison	Bob Russell
Mrs Ann Cryer	Mr Gary Streeter
Mrs Janet Dean	Mr David Winnick

Witnesses: **Mr Richard Thomas**, Information Commissioner, **Mr David Smith**, Deputy Commissioner and **Mr Jonathan Bamford**, Assistant Commissioner, Information Commissioner's Office, gave evidence.

Q1 Chairman: Good morning, Mr Thomas. May I thank you and your colleagues very much indeed for coming this morning. As you will know, this is the first evidence session of a new inquiry for the Home Affairs Committee with the title: A Surveillance Society? We are very pleased to have you with us today to open the evidence session. I think it is probably quite rare for this Committee, and probably many other parliamentary committees, to take as the title of an inquiry, the theme of an inquiry, a single report produced by somebody in your sort of position. We felt that the issues raised by the report you published a few months ago were sufficiently interesting and challenging that we should give greater attention to them ourselves. We are very grateful to you for that; and also for sharing a little in advance with the Committee the report I know you have published this morning. I wonder if we could start with you introducing yourself and your colleagues for the record, and then I will open the questions.

Mr Thomas: Thank you very much, Chairman. I am Richard Thomas, the Information Commissioner; on my left is David Smith the Deputy Commissioner; and on my right is Jonathan Bamford, Assistant Commissioner specialising in this particular area. May I start by just saying how much we really welcome the inquiry which this Committee is launching. Above all, when we published our report last year we called for public debate, and I think this Committee is exactly the right place for that debate to take place. We have provided the Committee with an updated version of that report, with a new chapter which we published today. I think that has been sent to the Committee in advance. That is the report of the Surveillance Studies Network which we commissioned. It is not our report—we commissioned it. We have supplied you with a memorandum for this morning's session setting out some views of our own. I would be happy to elaborate on those during the course of this morning. What I would say is that, to a large extent, we were trying to create a wake-up call: the march of technology; political imperatives; commercial impetuses; a whole raft of drivers moving towards greater surveillance of the population. The report contains examples of what surveillance meant in the year 2006, when it was written. It also rolls forward to 2016, 10 years on, looking at technology in the pipeline; looking at various developments, all of which were sourced in that report. This is not science fiction. This goes into factual situations. It is also a lot more than CCTV. People focus on cameras in the street and think that is what surveillance is all about. We are very keen to talk about the electronic footprint which people leave in their daily lives: the collection; the sharing; the use of personal information. Every time you click your mouse, you make a phone call, use a payment card, drive your car or whatever, there is potential surveillance there. The report and certainly I, as Commissioner, are very keen to emphasise the benefits of surveillance. This is not a one-sided debate; this is a debate about balance and where lines should be drawn. We are very clear, in our own submissions to you and the report we have published, that each individual initiative may well have very well intentioned benefits in terms of the security and the safety of the public; and in terms of improvements to public and private services providing quicker, cheaper and a wider range of benefits to the public; so there are very clear benefits. Also, and I am sure we will be elaborating this, this morning, we believe it is important to recognise that there can be risks. There can be risks to individuals, and we will elaborate on that; and there can be risks to the fabric of society as a whole. Again, we would like those to be explored. I think the fundamental question which we posed in our report, and your inquiry is now posing, is: are we moving towards some sort of surveillance society, where technology is extensively and routinely used to track and record our activities and our movements? We would say, yes, there is a growth in such activity; and therefore there is a need for the public to be aware of what is going on; there is a need for a rigorous debate, particularly where these techniques are not obvious—they are invisible, or people are not aware of what is going on. We need to move towards some sort of political consensus as to where the lines should be drawn; what safeguards are needed; and how they should be applied in practice. I hope that gives you an oversight,

Chairman, of the issues we are addressing. We are very happy to take the questions you would like to put to us.

Q2 Chairman: Thank you very much indeed. Can I start by asking you a very straightforward question about what it is that we should be concerned about? Is it the practical effects of the misuse of data; or is it the more philosophical objection that just, in principle, having so much data held about ourselves in some way infringes our sense of being free citizens in a free society?

Mr Thomas: I think it is both. There are some real practical issues. There are risks to individuals; there are risks to the nature of society which we are trying to secure in this country. Also I think there are some more philosophical issues about the collection and use of information, and that tends to shade back into the previous debate about what sort of society are we content to live in? The practical risks are probably more in terms of the detriment to individuals which can occur when mistakes are made, for example mistaken identity; where there is false matching and the wrong individual is identified; where there is inaccurate or out-of-date information; where there are breaches of security. These, to a large extent, map on the data protection legislation. You will be aware, I am sure, of the European Directive and the UK Act of 1998, which is my responsibility to oversee. The fundamental principles of data protection match fairly well onto these sorts of risks and, I think, have stood the test of time pretty well. We can debate how well it is being applied. I think there are some wider philosophical questions, partly in relation to why we collect information in the first place. Again, that does map back into data protection, because that does require clarity as to purpose, and limitation of purpose and for people to be told usually why and how information is being collected. I think we see the accumulation of information as having a certain inevitability about it. I do not think we are going to be Canute-like trying to say, "No more collections of information". What we are saying is the importance of organisations, whatever their motivations, being very, very clear about the boundaries of what they are collecting and how they are going to use that, and being aware of the risks that things my go wrong.

Q3 Chairman: Is there a danger of over-egging the pudding by thinking up almost every issue you could be concerned about and saying, "Well, this is a product of the surveillance society"? I am struck in the report which you published this morning (and I should say that you commissioned this and these are not necessarily your views) that it talks about the surveillance society and says the results are that all too often police hotspots are predominantly in non-white areas, and supermarkets are located in upscale neighbourhoods, easily reached by those with cars. Leaving aside the debate about the choice of terminology of "non-whites" as opposed "to poor areas", which this Committee has been wrestling with over the last few months in a different context, what they are actually saying there is the problem is, because we have got surveillance, the police concentrate their efforts in the areas where there is most crime, and Waitrose put their supermarkets in posh areas. That seems an extraordinary sort of thing to link up and say, "This is all the product of a surveillance society". Surely we want the police to concentrate their efforts in the areas where there is most crime? Surely ever since Mr Marks and Mr Spencer first opened their market stall they had one eye on where their customers were going to be?

Mr Thomas: Going back to George Orwell and perhaps even earlier, it is easy to build up a picture which can be interpreted by some people as being paranoid or unduly concerned. I am very keen indeed that we should not do that. The report we commissioned did paint a fairly comprehensive picture. I think it is a very worthwhile contribution to a debate; but I am not going to be endorsing every last sentence or conclusion of the authors of that report. I think there are some very serious issues there. I talked about some of the risks to society, particularly where computers without human intervention are classifying, are sorting information or processing information. The risks I think can be very real and some of those are spelt out in the report. To take one quite controversial example, the police DNA database, or the database to which the police have access; that has grown really quite dramatically in recent years. There was some parliamentary debate, not a great deal, and I think the public debate followed that. My Office was not consulted as those measures were being brought forward; and we now have a situation where a significant proportion of the entire population has their DNA on that database and there are clearly benefits, and there are clearly risks there. The point I want to make is that the proportion of young, black males having their DNA on that database is 40% of all young, black males now. It could be said that is perhaps because they are involved in criminal activities.

Q4 Chairman: I do not want to intrude too much but we will come back to the issue of the DNA database in further questions. Perhaps you are conceding my point that it may be going a little bit far to say the police use data to concentrate their efforts where there is a lot of crime?

Mr Thomas: I do not think we are going too far, Chairman, but I think there is a risk that some people may go too far.

Q5 Chairman: Can I move on to my final opening question, which follows on from that. There can be a tendency in this debate to suggest that these problems you illuminate are essentially driven by the State or by big private sector organisations; that people are doing things to the public that the public does not want to happen. Is it not the case actually that some of the things that are happening are very much driven by public demand? I gave you two examples, and on the detail of CCTV we will come back to that very shortly; but most Members around this table will say that having more CCTV cameras

in our areas makes us more popular and not less popular. More substantively, the outcry after the Soham murders was that allegations about Ian Huntley, not proven convictions but allegations about him, unproven facts, were not made readily available to the school that employed him. The Bichard Inquiry, set up in the wake of a genuine upsurge of public concern, was essentially charged with making sure we had more efficient systems of spreading unproven information about individuals around the country and making that unproven information available to tens of thousands of potential employers. Surely those are two examples, and again I am not necessarily asking you at this stage to go into great detail of that particular case, of where actually the public are saying to politicians and saying to Government, "We expect you to put these systems in place; and if you don't put these systems in place you are letting us down"?

Mr Thomas: If I could answer your first question on CCTV and perhaps David, who is very close to the Bichard Inquiry, could pursue the second point in more detail.

Q6 Chairman: Particularly on where the impetus is coming from. The technicalities of it we can go into, but the impetus is not coming from the public.

Mr Thomas: I will start with the general proposition that, by and large, people value their own privacy very significantly indeed. They want their own personal information safeguarded to a great extent—we have research demonstrating that. They are rather less concerned about other people's privacy and other people's personal data. I think that is probably one of the dilemmas we face. Secondly, I fully accept that there is and has been for some time strong demand for CCTV. Our own research confirms that; and we are very mindful of that. When it gets on to even more extensive use, our report demonstrates we are already the most watched nation in the world in terms of numbers of cameras per head of population. I think there are over four million cameras and one camera for each 14 members of the population. I think our line is that is fine; there is a demand for that; but people are a lot less happy not knowing what is going on. Transparency is very important; and that is why the Data Protection Act does encourage, and sometimes requires, openness, labelling as to where cameras are, what they are being used for and what their purposes are.

Q7 Chairman: I am going to cut you slightly short on this—we will come back to the detail. Do you concede my fundamental point that quite a few of the things that Government is putting into place about data sharing and about CCTV is actually reflecting a popular demand?

Mr Thomas: In general terms I fully recognise that situation. I think sometimes it is important that politicians, commissioners and others stand up and say, "Just be aware of some of the risks involved".

Q8 Chairman: Mr Smith, would you agree, in the case of the Bichard Inquiry and those events, that that happened in response to a fairly broad public sense, which probably was not just driven by the media, that something needed to be done, and the information needed to be more widely available?

Mr Smith: The Bichard Inquiry into the events after the Soham trial are indelibly imprinted on our memory for life. I think there are a number of points to bear in mind, without going into great detail about the case. After the trial data protection was blamed essentially for the information not being shared and for the consequences in terms of the murders. Deeper investigation showed that not to be true. The information was available and should have been shared. It was the systems that fell down. It was not a question of more information needing to be made available; the system that was there did not work. You are absolutely right, Chairman, that there was pressure for more sharing of information. The Bichard Inquiry brought about a new system to enable police intelligence, as well as conviction information, to be made available, quite rightly. There is much to be commended about the system that is now in place; but we remain convinced that we could have had a system that protects children just as well with less impact on individuals' privacy; without things like shoplifting convictions that people had when they were teenagers coming out 15 years later when they apply for a job. It is a complex problem, and the solution is not sophisticated enough. We could have done better.

Q9 Chairman: That is helpful. I think we will probably come back to some of those issues again.

Mr Thomas: I think it was Benjamin Franklin who said something like. "Those who lightly give up their liberties in the name of safety, deserve neither safety nor liberty". I think there is a certain truth in that observation.

Q10 Mr Winnick: Mr Thomas, there is a great deal of concern, and understandably so obviously, about the amount of information the Government, whichever Government happens to be in office, holds about us in government departments. Is there not an equal danger, and some may say a greater danger, on the information which is held on so many people, literally millions of people, in the private sector? What would you say to that?

Mr Thomas: I think, Mr Winnick, both areas are important and there are some overlaps and connections between the two. You are quite right to say that vast amounts of information are held on each of us in the private sector, in the financial area, in the retail area, loyalty cards and the credit reference agencies. In those sorts of areas a lot of information is held about us, as is held about us in various public sector bodies. What I would say is, in the private sector there are pressures to get it right which do not necessarily always exist in the public sector. We have had some engagement with banks recently. We have been very critical of them for the way they have been careless with people's personal records. We have secured undertakings of good

behaviour from 11 banks, and we named those banks; and this shot right up the agenda to the chief executive level of those banks taking us a great deal more seriously. There are commercial pressures which do not necessarily exist in the public sector arena. There are political pressures in the public arena, but one of our missions, if you like, is to bring what is going on more to public attention so there can be a greater debate. There is another set of questions which may follow later about the extent to which the public sector, whether it is the police or the tax authorities, should have access, for example, to financial records, health records or to credit reference bureaus. Many debates are going on about public sector access to private sector data bases.

Q11 Mr Winnick: The Financial Services Authority, and I am quoting directly, says: "If you're an adult living in the UK, it's almost certain your name and details are held in the files of the three main credit reference agencies", and names those agencies. Somewhat disturbing?
Mr Thomas: It is not remotely surprising, Mr Winnick. I think it has been the case for probably 15 or 20 years now. Experian, Equifax and Callcredit are the three main agencies in this country and, yes, indeed, they do hold quite detailed personal information.

Q12 Mr Winnick: They would have information about everyone in this room?
Mr Thomas: Almost every adult. The electoral roll is the foundation of much of their work, and they hold a great deal of information. We regulate that very tightly. It was originally regulated under the Consumer Credit Act; it is now tightly regulated under the Data Protection Act. We have our issues from time to time. My predecessors some 10 or 15 years ago took the bodies to the tribunal and served enforcement notices, and we moved them away from some of their unacceptable practices in those days. For example, keeping information by address now is kept by reference to each individual. They do work very hard to make sure they follow the rules in terms of accuracy, corrections and keeping it up-to-date. We do have issues from time to time and when we get complaints and we deal with those as they come in.

Q13 Mr Winnick: The electoral roll plays quite a major part?
Mr Thomas: Yes, the rules were changed in 2002. Now you can in effect opt out of having your electoral information used for commercial purposes. There are some detailed limitations on that.

Q14 Mr Winnick: Is that sufficiently well known, would you say?
Mr Thomas: I think so. We had a lot of complaints about nine months ago about a website which was called B4U; and that was available to the general public allowing people to trace other people in this country. We had very large numbers of complaints, not least for example from policemen and prison officers who did not want to be traced. This website B4U was using pre-2002 electoral roll information. We took a very strong line against that; we served an enforcement notice and that activity has now stopped. We are vigilant, Mr Winnick, to deal with those sorts of problems as they surface.

Q15 Mr Winnick: Do you think there is sufficient recognition that when one signs up for whatever it may be, a store card, or agreeing to a loan, to a large extent we are really signing away our privacy? Do you think there is this recognition of the dangers involved?
Mr Thomas: The data protection legislation requires that people be told what information is being collected and how it is going to be used; but I am the first to recognise that people do not always read the small print sufficiently and do not fully understand. I wrote a publication over 20 years ago *Plain English for Lawyers*, and on the back of that I have been working at international level to take a much, much more transparent and user-friendly approach to what are called "fair processing notices". We are working with the Americans, Europeans and others to have a much more global approach to putting clear information upfront and not littering the information with detail which people do not want first time round. It is what is called a "multi-tiered approach". I recognise that it is an ever-going battle to make sure people do fully understand, not just when they sign up but also through the media. By far our most popular leaflet is the one about credit reference agencies; we pass large numbers of that out every year. It is an uphill battle to educate the public as to how their information is being used in that environment.

Q16 Mr Winnick: It must be quite an uphill struggle. I do not think anyone doubts that for one moment. You indicated some of the safeguards of the electoral roll post-2002. Do you feel that we should limit far more the ability of private agencies to demand personal information? Some of the personal information is very extensive indeed. This is the first session, as the Chairman has said, of this inquiry and there will be many, many witnesses I am sure from the private sector as well. Do you feel there is a case at this stage to limit the amount of information that these agencies want?
Mr Thomas: We tend not to be interventionist in the sense of prohibiting activity. To a large extent the data protection rules regulate how information is to be collected and used. With some exceptions; they do not normally prohibit altogether the collection of information. If I can go back to credit reference agencies, I think they do serve an important role in the credit-granting process. We have got fantastic amounts of money being borrowed; unsecured and secured loans; and that economy could not happen without the existence of the credit reference agencies. They do serve a very important role to ensure responsible lending and responsible borrowing. That is a debate for another committee.

Q17 Mr Winnick: Obviously this is their argument. I am not dismissing their argument for one moment.

Mr Thomas: I speak from personal experience, Mr Winnick. I was the Director of Consumer Affairs at the Office of Fair Trading in the 1980s, so I had clear insights into how the credit market worked. I do think there is merit in the argument that you need information about your borrowers in order to engage in responsible lending. It is not an absolute argument and, as with so many things, frameworks are needed; limitations are required.
Mr Smith: Perhaps I could just add that we have had from time to time discussions with supermarkets about loyalty cards and the information that is collected there. There is one issue we have been particularly keen on which is not to make people believe that they have to answer questions in order to get a card. You have to give your name and address to get a card but, in simple terms, you do not have to tell them whether you have a cat or a dog. They might like to know that information but it should be clear to you that it is your choice as to whether you answer that question. I think the other thing about areas like supermarket loyalty cards, is that it is not written but there is perhaps an unwritten contract between Tesco or Sainsburys and their customers so that when you give this information you have an idea of what is going to happen to it; and you have an element of trust. We have had discussions with some of the supermarkets about where that has been threatened. It is commercial drivers that drive them. They do not want to upset their customers. Their loyalty card information is a very, very valuable commercial product. They do not want other people to get their hands on it, because they will use it in competition. There are drivers in the private sector which, if you like, assist data protection compliance which are not necessarily there in quite the same way in the public sector.

Q18 Mr Winnick: If you take, for example, the building societies, not for loan purposes but for various savings schemes they have, their questions in the main are very intrusive indeed; obviously on the financial side, as one would expect, it would not make sense otherwise; but when it comes to questions of marriage, divorce, who you live with, children and so on those questions seem extremely intrusive indeed?
Mr Thomas: I think we are getting a little away from our agenda. All I would say is, I think those sorts of characteristics feed into credit scoring techniques, because the credit scoring techniques are based on such matters as your stability and your characteristics which show whether you are going to be a high risk or a low risk. If I may say so, I think we are getting a little far away from my data protection role.

Q19 Mr Streeter: Do you have the power to go into credit reference agency database at will and pick out a random file to check out that they are keeping information correctly?
Mr Thomas: No, we do not. David and Jonathan will say a little bit more about the detail of that. If we want to "assess", to use the legal wording, the processing of personal information, whether by a private or a public body, we have to have the consent of that organisation. We have said in our written evidence to this Committee we think that is not acceptable. I think we would be urging you to look at that more closely; because I think that is wrong for a regulator. Trading Standards, the Office of Fair Trading, Financial Services, Food Standards, Environmental Health, all these sorts of bodies have the power to go in. We have a search warrant power, but that is rather nuclear; that is to go in and seize a particular document or a particular computer when we suspect there has been a criminal activity. That needs a judge's warrant. For the most part, we have to work closely with those we regulate and we seek their cooperation. We take a line which is: to be constructive; to help them get it right; but we do feel that we need to have the teeth there. The teeth both deter in the first place and also allow us to make sure things are being done correctly in practice.

Q20 Chairman: When you sign up to something like the loyalty card it is compliant with the Data Protection Act; but essentially you sign up to all the purposes that the company has told you they wish to use your data for. I may want to have a loyalty card; I may not want my supermarket to analyse the data that they get from the loyalty card in order to plan where they want to open another supermarket and perhaps ruin the shopping in a market town. Should we have more choice as consumers about whether we want to volunteer all the data that is being taken off before we sign on the line and sign away our privacy?
Mr Thomas: In principle my answer is a clear, yes, although I think some supermarkets do not actually require your name and address. You can have a loyalty scheme which is anonymous. You spend so many pounds each week and you get the points and you get the rewards; you do not need to have the personal details at all and in that case that is fine. I am not aware of any supermarket which offers a two-tier approach—a card with personal details and one without, but that is conceptually quite possible. In principle my answer is a clear, yes, choice is good for people.

Q21 Mr Winnick: Mr Thomas, there is another aspect before leaving this particular section, and that is the way in which a Government intends, as it would say, to combat criminality, or prevent criminality to get information from the private sector. That would be the argument government departments would state. I know you have made some comments on this. Is there not a danger of the two combining which would indeed be a threat to civil liberties?
Mr Thomas: Yes, there are risks, Mr Winnick. The Serious Crime Bill is going through the House of Lords at the moment but has not yet come to the Commons. This issue arose during the committee stage and I was invited to meet peers from all parties about two or three weeks ago. That does have a provision in it which will allow greater access by law enforcement bodies to private sector data, particularly in the area of fraud. First of all, we are

very pleased that now in the Bill there is an explicit statement that all this must be in line with the Data Protection Act; secondly, the Government I think are still considering how best to achieve this; but we have been pushing (and I think it is accepted broadly in principle) that there will be a code of practice on which we will be consulted to regulate the public sector access to the private sector databases, including to any anti-fraud organisation. Also the Home Office have accepted in principle that we should have the power to go in and inspect. I mentioned to Mr Streeter that we do not have this power—sometimes we negotiate for it, whether in return for an undertaking, as with the banks exampled earlier; but in this situation we have now got the Government to agree that we should have that power written, not into the statute—I think they are still considering that—but if not in the statute, in the code of practice. You are absolutely right, there are issues, there are risks and, as with all these areas, we need a framework to make sure that the legitimate purposes of the police and the law enforcement bodies are served by accessing this data, but it is not a free-for-all; they cannot just go in and look at everyone's data and just make merry with it; it has to be targeted, proportionate, for a defined purpose.

Q22 Mr Winnick: With the concessions the Government has made, which seem very welcome concessions, you are far less worried, are you?
Mr Thomas: Less worried than we were originally. We have had constructive dialogue with the Home Office since the middle of last year on this subject, and we put the flag up, as it were, as to what our concerns would be. As with so many of these things, they are not absolute; there is no black or white; but we do feel that the movements now being made will go a long way to satisfy our concerns.

Q23 Mr Winnick: To a large extent due to the interventions that you make, presumably, or your office?
Mr Thomas: On that one we are pleased. As always, the proof of the pudding is in the eating. Let us see how it works in practice.

Q24 Ms Buck: Can we just go back to the CCTV discussion we were having earlier. You gave us some very striking figures, and the report includes more: 4.2 million cameras and the chance of an individual being caught on 300 cameras a day. I think that was quite a depressing statement you made about people's attitudes to CCTV and the relationship between their privacy and other people's privacy. What steps do you think can be taken in public policy to advance that debate so that we are able to have a proper and balanced debate between the benefits which are, to say the least, unproven, on CCTV, and in respect of privacy?
Mr Thomas: Could I start by saying that it is not just what I might call "conventional cameras". We are now moving into new technology: digitalisation where ANPR is already being used—automatic number plate recognition; and facial recognition technology is being used. There is the capacity now to have very, very small cameras; and the report suggests, if the political will was there, they could be buried in lampposts and no-one would know exactly where the cameras were. In terms of the public debate I think, first of all, we would always want to see a rigorous debate about the benefits; and I think the jury is still out in some respects. I recognise entirely that the population like cameras and cannot get enough of them; but I think the Home Office research has indicated that there is still some doubt as to their efficacy in both certainly preventing crime, and also debates about their role in detecting crime. They do give public reassurance and I would not want to dismiss lightly the need for the public to be reassured, because perceptions can be as important as reality in this area. Assuming that we are going to stay with large numbers of cameras for the foreseeable future, then I would certainly want to push the transparency button very hard indeed. People should know where the cameras are. We have been wholly against hidden cameras, unless there is extremely good reason in very, very limited circumstances. We want maximum transparency. I am not certain we are looking for a label on every camera; particularly for roadside cameras that is not realistic; and we will share some thoughts with you about how that might be addressed. We also would be hostile to the suggestion of any sort of microphones associated with cameras. There is a debate starting now as to whether there is a case for the authorities to place microphones on the streets, and our instincts are very, very hostile to that idea. We think that would be unacceptable. There is a debate also which has started in the last couple of months about loudspeakers associated with cameras saying to people, "Pick up that cigarette packet"; or, "Behave yourself". I think Middlesbrough have been trialling this, and a number of other local authorities have now received some Home Office funding to go down that road. That may be a bridge too far; we will have to see how the public react to that. We are certainly not enthusiastic about that sort of approach. On the siting of cameras, Jonathan will have interesting ideas to share with you.
Mr Bamford: As the Commissioner has made clear, I think transparency is important. The public needs to have confidence in what is happening in terms of surveillance that is taking place. One of the difficulties that we do have in the data protection world occasionally is when we talk about different sorts of technology which actually starts to capture information about people—in this case imaging technology. How do you apply the normal sorts of data protection rules, which perhaps we touched on earlier, such as explaining to people when they sign up for a loyalty card where they can see a nice little declaration there and make some choices? With cameras it is very different; you do not really have a choice about your image data being captured at that point. I think it is important there are signs that at least alert people to the fact that image-capture is going on and giving them a chance to find out who is involved in that because it is not always obvious, particularly in town centres; shopping centres are

owned by different people than the public anticipate. A particular challenge is when we talk about the road network because as motorists, as we drive along, we might see some signs there which warn us about cameras but do not really tell us who is involved in the monitoring as we go from one police force area to another; whether it is the Highways Agency; whether it is Transport for London potentially, or anybody else who might be involved in automatic number plate recognition capture. Maybe we need to be slightly more creative there in trying to actually come up with solutions which help the public work out who is involved in the surveillance. One simple solution might be to create a website which has the road network on it; we are all used to mapping technology now, route planning; and you could click on that and actually find out who is involved in the surveillance at a particular point in time. That would cover mobile cameras and those sorts of aspects. I always thought of it in our office as something like www.cameras.gov.uk where you would not have to convey much on a road sign to allow somebody then to exercise a little more in terms of their rights to find out who is involved in surveillance. I am not saying monitoring should not go ahead, but more should be done to regularise it in some way. I think the other thing we would say as well is, transparency is all well and good; it is important as individuals we are aware of what is going on; but to come back to the other point about the growth in CCTV and the public's insatiable demand apparently for this, I think of the things that we are going to make clearer in our revised CCTV Code of Practice, which tries to make sure that CCTV-based surveillance operates in accordance with data protection law, the thing we will emphasise is the actual assessment procedure, in deciding whether to establish a scheme, should be very, very rigorous. It should not just be on the basis of public popularity, or the technological capability to do it, or the financial capability to do it. What you have really got to look at is: is this really proportionate to the evil we are trying to address here? What are we trying to deal with by having CCTV cameras? Will they actually do the trick in addressing that? If we are worried about street crime near tube stations, would better street lighting actually be much better than putting in CCTV cameras? We need a proper assessment methodology there to decide in the first place whether this should go ahead. The judgment may well be, yes, that is a proper technology to use and is a proportionate thing to do; but based on that then you actually come to what are the safeguards that should be in place in terms of how do we make the public aware about this? How do we make sure that the images are of the right quality?

Chairman: We have a large number of questions to get through. Please do not try to hang the answer to everything you want to say about a particular topic to the first question.

Q25 Ms Buck: To go back to a particular point I wanted to pursue which is the development of CCTV and the improvements in imaging technology and the fact that there is a debate now about the police looking for consistency in CCTV imaging in order to be able to make use of that technology for themselves; there are clearly risks inherent in that, and you have outlined what they are. A number of my constituents would no doubt say, "What on earth is the point of having any of this technology at all if it is not able to be used by the police; if it is not able to hone in on, let us be frank, conversations, number plates and face recognition"? How do we overcome this conundrum; that people only want the surveillance technology, if you like, if it is going to be highly effective; and yet simultaneously want to be assured of their own personal protection from that very surveillance?

Mr Bamford: I will go back to the answer that I was providing, which actually says it is all about safeguards at the end of the day that actually provide the public reassurance; and we need proper standards therefore to make sure that if the public is happy that their lives are intruded into in some way by surveillance that the images are sufficient for the police to actually identify the perpetrators of a crime. The idea that you have to send your CCTV images off to NASA to have them processed so you can identify people is clearly ludicrous. From a data protection point of view our law says that personal data has to be adequate for its purpose. We would argue that if you are going to have CCTV cameras, make sure they are fit for the job basically. We want to drive up the standards of the surveillance that is justifiably there, in terms of CCTV imaging, but making sure it takes place in a context of where it actually does make a difference.

Q26 Ms Buck: The implication of this is that you are not satisfied with the safeguards that currently exist, whether that is in data protection or a code of practice. Is that what you are saying? Do you believe that there is a difference between the safeguards and the use of surveillance technology and CCTV in the public sector, effectively the crime-fighting technology, and in the use of private cameras?

Mr Bamford: Clearly the development of CCTV surveillance has been across both sectors really. There is a lot of public money being put into CCTV surveillance, and we should be begging the question about whether we are getting value for money with some of the schemes that are there, enabling them to go on. The use of that information can be wider than, say, a limited private sector scheme. I think we need to be concerned in terms of how much imaging data is caught and what purpose it can be used for, and whether there is an element of function-creep, if you like. It is like automatic number plate recognition; the idea of denying the criminals the road seems a very sensible idea. If you are matching number plates with vehicles that are wanted by the police for a variety of reasons, people who are wanted who own those vehicles, you can see how that works in real time when somebody is detained very quickly. Now, because of technology and storage capacity increase, should we keep the automatic number plate recognition records for five years, three years or two years? We move along by degrees to something which is rather different than

we started out with, which is the idea of spotting a vehicle immediately and taking action in relation to it. They then say, "It'll be handy to keep this for longer". In the public sector you have got a real issue about that. In the private sector we do see invasive technologies being used as well. Automatic facial recognition can now be deployed by private sector organisations. We have heard instances of saying that might be helpful in identifying people who often turn up at the returns desk of major stores because people who bring back clothes a lot maybe did not buy them in the first place and stole them, and they are trying to get credit notes for something they do actually want, or are trying to get money back. If you spotted all these people coming back then somehow that would enable you to run your business better. There are lots of people who do not like trying on clothes in shops, like me, who take them home, try them on and bring them back and worry about maybe being labelled as a shoplifter.

Mr Thomas: The underlying theme is public confidence. It is not about the exact boundaries of the law; it is: are the public confident in the cameras? If they go too far and microphones are deployed and the public really reacts against that then that is going to serve in no-one's interest.

Q27 Ms Buck: What you have been saying so far is that there does not appear to be any great sense of the public being concerned about the use of technology insofar as other people are concerned; hence the demand for surveillance cameras which are hugely popular. To play devil's advocate, the fundamental question is: if you are innocent, what have you got to fear?

Mr Thomas: It is a very, very familiar argument to anyone concerned with privacy, and David has been in this area for 15 years or more and is itching to answer that particular point. I think the general point is that you can always go on more and more with surveillance. You could say we could stamp out any form of crime or anti-social behaviour by having cameras in everyone's living room; where do you draw the lines? It is not what technology or what law enforcement could be doing; it is what is acceptable in a modern democracy.

Q28 Chairman: I have been listening to this discussion for some time and I have not yet heard a single example given to this Committee of somebody who has actually suffered as a result of the introduction of this technology. It may or may not work; it may or may not raise issues of principle; it may or may not be a good investment of public money.

Mr Thomas: You could be saying, Chairman, we are doing a wonderful job!

Q29 Chairman: We could imagine all sorts of things that may be going wrong, however we do seem to be a little short of examples, despite there being 4.2 million cameras, of people's lives being ruined by this technology.

Mr Thomas: You have not asked us yet. We can give you many examples of people who have suffered detriment as a result.

Mr Smith: There is one very well known case, Chairman, the *Peck* case which went to the European Court of Human Rights where an individual was photographed on the CCTV camera essentially in what was a semi-private area, in a car park. He was trying to commit suicide and these images were essentially broadcast, I hesitate to say, for public entertainment. The European Court of Human Rights found against—it was a local authority in this case. The images were essentially used for a different purpose. There are areas which go too far. This is this question of purpose. I think it comes back very much to this. With cameras that listen in if you are talking of targeted police investigations, there is an area where you know drug dealers meet and you put a listening device in, that is targeted and that is okay. What if we are then talking about shoplifting rather than drug dealing? Is it okay to use that information for that lesser crime? If it is okay then, is it okay to put listening devices in anywhere to detect shoplifting? Where do we draw the line? I do not think, Chairman, we have any answers and we are not pretending we do. I think we can say to you that the public accepts CCTV cameras in public areas. I think we can probably safely say they would not accept cameras and listening devices in their living rooms. Where is the dividing line? We do not know but we are getting nearer to it.

Q30 Ms Buck: How can you help us to construct a framework for a policy debate that allows government and the public to discuss where those lines are drawn? At the moment, I think it is extremely difficult to be able to frame that debate. I think we really need to be able to pin that down.

Mr Thomas: On cameras and related issues, we will send you the updated version of our code of practice during the course of your inquiry. The existing code has been there for about seven or eight years now. It is out of date. We are moving rapidly now to finalising the updated code. I am afraid it is not ready for this morning but we will share that with the Committee, if you would like that, as soon as possible. That will set out our approach. It will have some clear dos and don'ts and it will be our attempt to apply the more principled debate we are having this morning to the practicalities of camera deployment. We can give you many examples in the area of database problems where people have suffered as a result of information either being incorrectly on a database or being used inappropriately.

Chairman: Thank you very much.

Q31 Mr Clappison: I heard you a moment ago drawing distinctions between different types of criminal activity and the extent to which you would allow use to be made of information technology. You did not mention terrorism in that. I hope you would take full account of the huge public interest in dealing with terrorism and the serious detriment

there can be to the public from that. Will you be giving it a lot of leeway, given what we hear about the scale of the problem?

Mr Smith: Terrorism is, if you like, the highest in the scale, but there is still a question, even with terrorism, as to how far you go in intruding into the private lives of everybody in the country in order to fight against terrorism. In everything there is a question of proportionality. A greater degree of intrusion is proportional in fighting terrorism than is proportional in fighting shoplifting.

Mr Thomas: There are some important exemptions on national security and law enforcement in the Act. We fully respect that. This is not a popular or easy thing to say, not least after yesterday's trial—we recognise the cross-over on this debate—but, sometimes, when the threats are the greatest, the need for safeguards is the strongest. Liberties are involved here. We are going to come on later, I am sure, to talk about privacy impact assessments. I have with me a pamphlet from the Department of Homeland Security which is right at the front of the American fight against terrorism, and they are taking privacy and safeguarding that extremely seriously. Worldwide, there is a recognition of a balance. Yes, the fight against terrorism is paramount, but, even there, there has to be some framework to make sure the authorities do not overstep the mark.

Q32 Mr Streeter: It is a fascinating debate. I am going to ask you a couple of questions about information sharing between government departments, but before that I would like to ask you a question, because I have not quite got to the bottom of this in my mind as I am listening to you speak. I know you are ruled by a couple of statutes, but do you have in your own minds a kind of golden rule or overarching set of principles which is your compass. Surely your job is not just about getting the balance right. Do you have a golden rule?

Mr Thomas: We have a way of reconciling the Data Protection and the Freedom of Information Acts that says we exist as a statutory independent body to improve public access to official information and to protect your personal information. I recognise that is very general. Going down a stage further on the data protection side, I would articulate it in terms of a society where there is proper respect for the integrity of people's personal information, where there is proper respect for their privacy, where people, as far as possible, know what is being done with their information and how it is being used and there are safeguards in place. I reinforce the point I made earlier, Mr Streeter, that it is not to prohibit activity; it is to regulate it. Please do not forget that data protection has its origins in Continental Europe, and in the 20th century in Western Europe and Eastern Europe. Some of my colleagues, as Commissioners in Poland and other countries, have seen the real evils of a surveillance society and they talk to us about those within their recent memory. Data protection has its roots in a human rights concern, not ever, ever to achieve in Europe or elsewhere that sort of environment again.

Q33 Mr Winnick: There is a film about that.

Mr Thomas: *The Lives of Others*, yes—a sort of data protection film.

Q34 Mr Streeter: Government databases, information stored about us. Could greater use be made of personal opt-ins and opt-outs without undermining the whole reason why it is important that information is stored about us by government departments, do you think?

Mr Thomas: I think you have to start the debate by recognising that there is a lot of pressure now for more information to be shared across different parts of the public sector. Sometimes that is not particularly controversial or not particularly difficult. In relation to the sharing of information between the tax people and the social security people, most of the population expect that goes on already. That would not be at all difficult. The sharing of information between the tax authorities and the police authorities, or between the health authorities and the police authorities raises far more controversial and difficult issues. I am not being at all evasive but you have to take a case-by-case approach. There is a Cabinet committee looking at these issues. We are pleased we have been asked to contribute to that. There are visions and statements coming forward all the time in that area. I think our input has been welcomed and we are putting forward a so-called framework code of practice, a code of practice overarching all these different initiatives, trying to set out some of the principles in the sorts of terms I have been sharing with you this morning as to what is clearly unacceptable, what is okay and how to approach the middle territory. We are hoping that this code of practice will influence the specific initiatives where information is going to be shared more regularly. On your specific question of opt-ins and opt-outs, it is not normally going to be very easy. I do not think government is going to be wanting to go down this road, because it is not like in the private sector where you do have a genuine choice: you can choose that holiday or that loyalty card or that bank account and you can shape your choices according to what is on offer. When you are dealing with the Health Service, the police, the taxman, by and large there is not much scope for choice. Having said all that, in particular areas I think there will be scope as you go forward for more to be expressed by way of preferences; particularly, for example, in electronic health records. That is a massive subject which your sister committee, the Health Committee, is looking at. We shall be coming forward there shortly. It is a very challenging area in terms of privacy, in terms of safeguarding information. There are all the benefits of sharing information between doctors and hospitals and specialists—and I am the first to recognise the benefits—but the risks are also very great indeed. There may be scope within that. We

are exploring with Connecting for Health the scope within that to tailor people's use of patient information more in line with their personal preferences.

Q35 Mr Streeter: As an aside, Chairman, it might be appropriate to get a member of that Cabinet committee to come to this Committee to give evidence. I was not aware of perhaps the new season of government information-sharing which is about to break out. In relation to the Government's Child Index, you have made some observations to the Government about that. Could you explain your thinking. Do you think such an index should relate only to children at risk and not to all children? I think I agree with you but it would be helpful to have an explanation .

Mr Thomas: Could I pass that one to Jonathan.

Mr Bamford: It is a very, very emotive issue when we start talking about children and what is best for children. One of the things that has perhaps been flagged up in the report by the Surveillance Studies Network and other research that we have commissioned specifically on children's databases is that we have moved much more away from just child at risk issues to child welfare issues more generally and trying to improve life chances. That has pushed us along to more and more information being gathered about children. During the lifetime of the Children's Index its ambitions started out as rather greater and have fallen backwards a little bit into being almost like an index of children and those practitioners who have an interest in children, so it is more limited than perhaps our original concerns would be in terms of data content. I think our philosophy has been that if we are particularly dealing with issues to do with children at risk, it is already difficult to find that information. We often use the phrase: if you are looking for a needle in a haystack why do we keep building bigger haystacks all over the place? We want information of the right quality relating to the people who really need care and concern attached to them, where people should take seriously the responsibilities in respect of those children. The simple acquisition of more and more information does not actually mean that people make better judgments. They will become overloaded. We have certainly heard it said from those who are involved in the early child welfare issues that sometimes it is more social workers we need rather than more information because we already have that much information we cannot act on. From a data protection point of view, we beg the question: Does the information that you say you need really make a difference? If you are keeping it, is it going to be easy to keep it up-to-date? The more and more you keep, the more problems you have in keeping information up-to-date, and the more and more you keep, the greater the collateral impact if that falls into the wrong hands. A data minimisation concept is something that we are quite keen on.

Mr Thomas: Going back to your question, I am quite, quite clear that the case for an index of children is very much greater for those children who are, or who are perceived to be, at risk, than is the case for a universal database of every child in this country in the more nebulous name of promoting their social and educational welfare. I think the second part is a great deal more doubtful. I stand by the views I have expressed on that.

Q36 Mr Streeter: I would certainly agree with that. Finally, you touched on this, Mr Thomas, in your opening remarks to me. Do you think there could be more benefits if more government departments shared data than they currently do; for example, HMRC and social security? How could we also safeguard the public if that were to happen?

Mr Thomas: There are benefits—and I am the first to recognise that—but also risks. I am sorry to be boring but it is a point I have to keep on making. We had some debate with the Audit Commission. They have a thing called the National Fraud Initiative to identify individuals who, for example, might be employed by a local authority at the same time as unlawfully claiming housing benefit. We had some concerns about the way they were using data-matching techniques and data mining. With hindsight, I think they would say they were going a bit too far. We had a battle with the Audit Commission which actually resolved itself in a very constructive way. We now have a code of practice which my office and the Audit Commission have signed up to which both sides are very happy with. Indeed, it will be not quite the template but the starting point for the wider code on information sharing I mentioned earlier. It is now held out as a very good example. Recognising the benefits, to go back to the point made earlier in another context by David: if you are clear what you are trying to achieve with data sharing, it is fine, but if you go too far, if you do not have the safeguards in place, you will forfeit public trust, you will alienate people and you will defeat the purpose you are trying to achieve. There was a report commissioned by the DTI about a year ago from the Council of Science and Technology. It said, if I can summarise, that with technology and sharing you can do almost anything these days but just because technology allows it to happen does not mean to say it should happen. There have to be clear political choices being made here and there have to be proper safeguards in place. Otherwise, you will forfeit public trust and confidence.

Q37 Mrs Cryer: Further to what you have just said, apparently your office have said that when the Identity Cards Act 2006 is implemented it should be consistent with the Data Protection Act 1998. Surveillance Studies Network believes that once ID cards are introduced the Government's reliance on those providing both technological and commercial expertise will increase. Could you say what implications you feel this will have on individuals?

Mr Thomas: A big question, Mrs Cryer, and I am sure the Committee does not want a complete re-run of the identity card debate. I was before this Committee I think three years ago.

Q38 Chairman: Certainly not, and I know Mr Winnick would not like it either.
Mr Thomas: It has been through Parliament.
Mr Winnick: My views have not changed.

Q39 Chairman: Nor have mine.
Mr Thomas: I did express strong views to this Committee and elsewhere. When the Bill was going through Parliament, I took the view that it was not right for me, as an appointed official, to engage in the political debate and the Bill is now the Act of Parliament. Now we are moving to the stage of implementation and we have had some dialogue with the Home Office and the Passport and Identity Service which will be rolling out that programme. That programme is going, I think, a little bit slower than perhaps had previously been suggested. We have concerns. Some of these are continuing concerns. We have concerns about data quality. Until it was announced, we were not aware that there was going to be a change of course. They are now going to be using information from the Department of Work and Pensions to populate the initial National Identity Register. Our concerns have always been the register behind the card. It is not the plastic card that causes the concern; it is the database. We have some concerns about the fact that the DWP has not had what one might call a completely clean database in the past and there are some anxieties about the data quality of imported data. We have always expressed anxieties about what is called the data trail. It can be an audit trail. We recognise there is a tension there, but the more that information is kept about every transaction with your card, every time your details are searched, the greater the risk in surveillance terms for individuals. That does begin to build up a very comprehensive picture, available to the state about your activities, which people may not be at all comfortable about. I think the controversy in more general terms will run for some time yet but we need to see how it rolls out in practice now.

Q40 Mrs Cryer: Further to that, still bearing in mind the introduction of ID cards, do you feel the data protection is adequate, or is there a need, or will there become a need for more specific powers to regulate different types of surveillance as technology develops?
Mr Thomas: I would like to invite my deputy David to say a little more about the role of the National Identity Register as a universal identifier, with the ability, not necessarily in practice, to connect together all the different schemes. To a certain extent, the fact that government and commerce are not joined up in practice provides some safeguards. If you have separate fragmented collections of information, ironically, from a citizen's point of view, that has certain advantages. It has certain drawbacks too but certain advantages. Whether using the National Identity Register or by other means, as you go down this route of drawing all the threads together then incrementally the big picture builds up. This is quite a subtle theme, and it comes out of the Surveillance Studies report. I do not think they are criticising us, but they say that we are looking at the individual schemes and giving red, green or amber lights to individual schemes, but are we sufficiently looking at the big picture and seeing how that is impacting on the citizen? The Government talks about public services being more citizen-centric, and that is welcome, but is anyone seeing it from the point of view of the citizen in terms of all this information being collected and shared about them? The National Identity Register could—I emphasise, could—undermine public confidence in this collection of information.

Q41 Chairman: Are you saying, in a sense, that the audit trail of when I use my ID card might perhaps be of less concern to me than would the state getting hold of my store cards and my credit cards, because if they had details of where I shopped and my financial transactions that may give the state far more information about me than the number of occasions on which I have identified myself.
Mr Thomas: I am not sure you could separate the two debates. If identity cards were used to prove your entitlement to drink in a pub at 18 years old or otherwise prove your entitlement to access certain private sector goods and services, then there could be a record of that transaction going onto the database. That would give the state more information about your private life but I think we are more concerned about the use of the national identity scheme in its dealing with the public sector, whether it is the police, the Health Service, the Immigration Service, Criminal Records. That is the main area of our focus and I think it will probably confuse the debate to worry too much about the extreme possibilities in accessing your purchasing activity.
Mr Smith: The Surveillance Studies report really paints a picture of a lot of developments, developed with good intention, for benign reasons in many cases, which, when coupled together, are starting to change the nature of the way in which we live. But they are isolated developments. The idea of an identity card and an identity number and a traceable database and this being used in all sorts of places, as Mr Thomas said, makes it much easier to link these different developments together. Even across the private sector—and it may be an extreme example—if you have one number used for tax purposes and the same number is available for your supermarket loyalty cards, the tax authorities could look at what you are spending your money on and see if that fits in with the lifestyle you declare in your tax returns. At the moment, one reason that does not happen is because technologically it is virtually impossible. If you put the same number in each database, it becomes relatively easy. It may come down to other reasons, but what was unthinkable because of cost and technology a few years ago is not unthinkable now. There is very little that is not possible. The public policy questions and the data protection questions come to the fore because the cost and the technological questions have disappeared.

Q42 Mr Clappison: Could I ask you a little bit more about access by different government departments to centrally held data. You have touched upon this already. You have mentioned what would be happening with the identity card and you have also mentioned public sector access to private sector information. With access by government departments to centrally held data, do you think it is properly dealt with in terms of regulation by the Data Protection Act?
Mr Thomas: The debate about surveillance is not unique to this country, by the way, the same debate is happening on a worldwide basis, but I think this debate reinforces the importance of the underlying data protection principles as a foundation to protect individuals. I have been Commissioner for over four years now and I was concerned that data protection had a rather mixed reputation, shall we say. It was seen as often a bureaucratic imposition. People were quick to hide behind data protection: "I can't do this because of data protection." We have all heard it in our different ways. I would be very keen to bring out—and I think the surveillance debate does bring out—the fundamental importance of such principles as accuracy, security, keeping information up-to-date and so on. I think it has stood the test of time. It has been developed in a way which is technology neutral, so, although we have seen fantastic changes in the last 20 years and I am sure we will see even more over the next 20 years, those basic principles are technology neutral. I think there is a much wider acceptance. Data protection is now seen as an essential safeguard against excessive surveillance and it does provide benefits to people. In some research about a year ago now we asked a question about people's social concerns. In rank order, crime was number one; education was number two; "protecting your personal information" came third in the league table. That was ranked by 86% of the population. It was way ahead of concerns about freedom of speech, ahead of concerns about the environment and so on, so people do care about it. If we had asked them about "data protection", I dare say it would be ranked much lower down the list.

Q43 Mr Clappison: Surely part of that public reaction will be protecting their details from criminals rather than use being made by central government.
Mr Thomas: As with any survey, it depends how you interpret the question. The question was put very broadly in terms of safeguarding your personal information. We had the same question two years running. My own office has exposed a wholly pernicious black market in the buying and selling of personal information. We published two reports last year and the Government is now going to legislate to introduce a custodial sentence to deal with that particular mischief. Yes, it is a problem. It has a read-over to the issues we are discussing this morning. The question we asked was cast in much wider terms about threats to privacy; that wrong choices and decisions can be made about you if people use your information in the wrong way.

Q44 Mr Clappison: I think in your answer you have implicitly accepted the conclusion of the Government's review on public services, that restrictions on sharing data can hamper the delivery of services. But you are saying that that can be addressed and there is this need for the safeguards in any case because of the issues of accuracy and so forth which you have mentioned.
Mr Thomas: The Government, understandably, said that if there is to be more sharing of information then we need to have stronger safeguards. They have talked about the role of my office but they have also linked that to the prison sentence for those who hack into the systems by impersonation or by payment.

Q45 Mr Clappison: Do you think the Government should be required to put in place codes of practice for information-sharing in the public sector?
Mr Thomas: I am not sure whether the question puts emphasis on the word "required". I think the Government is going down this road in any event and therefore there may not be a need for legislation, but I think that is a debate which could be had. There is almost a plethora of codes at the moment and one of our concerns is that there can be too much guidance. It sounds ironic but you come across situations—and the research proves this—where lots of people in the police and social services and health have drawers full of guidance: they shove it in the drawer and never read it. We are trying to have a more consistent approach. That is why I talked about the framework code which we are developing for public sector information sharing which could then be applied in a more targeted way in a particular environment.

Q46 Mr Clappison: You think that will be streamlining a lot of what is taking place in other codes of practice.
Mr Thomas: Exactly that. If there is not a maintenance of the current enthusiasm for codes of practice, then I think there may be a case for a mandatory requirement. I am not ruling that out but I hope, particularly with government, we can achieve that on a more consensual basis, because an imposed code is never one which is going to work. The whole point of codes of practice really is to get something which is going to work in practice which is achieved in a constructive spirit.

Q47 Mr Clappison: Coming at it from a slightly different direction, on the basis of what you have seen and your experience: other than creating a central database for use by public services, what steps do you think the Government could take to increase the efficiency with which it retrieves and uses data?
Mr Smith: I think we are getting close now to privacy impact assessments. I am not sure whether the questions are going to come on to that.

Q48 Chairman: We will come on to that later.
Mr Thomas: We see the privacy impact assessment as a really important way of addressing the particular question you put, Mr Clappison. The

fundamental message for me to send to a government department, a local authority, a police force is: Think before you act. If people think through what they are trying to achieve through the use of personal information, think through what the risks are, make sure they do not go beyond what is necessary, then I think we will get it right. But if people get sold a whizz-bang computer which can assemble lots of information and therefore will use it and just let anyone have access to that, then it is going to end in tears.

Q49 Gwyn Prosser: Mr Thomas, we have been talking about the general sharing of data across databases. I want to ask you specifically about tests and safeguards put in place when the police want to interrogate a particular database to progress their investigations. We have touched on these issues but do you think the present tests, present safeguards and assurances, are adequate?

Mr Smith: Much depends on what information it is the police want to access. We have the Regulation of Investigatory Powers legislation. That controls telephone tapping but it also controls access to telephone records and the like. We do not have any problems with that legislation. There might be matters of detail but the whole thrust, that the police have to do a proportionality assessment and check whether access is right in relation to the crime they are investigating, is correct. There are also exemptions in the Data Protection Act that allow organisations to give information to the police which, if you like, in ordinary circumstances they would not be able to give. Again, there is a similar sort of test as to whether enforcement of the law would be prejudiced if the information is not provided. I do not think data protection provisions then stand in the way of the police accessing databases. We are seeing more of the building up of collections of information. It is not information that people are holding for their business purpose and to which the police are getting access; the information is being held for policing for the first time. Telephone records are one example. Essentially, telephone companies may have needed to keep records for six months or a year, but partly through UK legislation, partly through a European Directive, there will be a time period for which the records are being kept beyond the business need of the telecoms provider, where they are a resource for the police if they would be useful to an investigation. With automatic number plate recognition, the simple approach to that would be to say that you set up a camera, you run the results against, say, the DVLA database and you stop people whose cars appear not to be taxed, so you do not need to keep the data—or you may keep it for a week or two, just to check. Now they are talking about two or five years so they can track back. That is what is changing. It is these big collections of information being held in case they come in useful.

Mr Thomas: We had a case recently where a 48-year old woman, when she was 14 years old, had been convicted of assaulting her careworker and had been given an absolute discharge. She discovered, because her neighbour was a policeman who improperly accessed the police national computer, a record of that conviction. It was true, it happened when she was 14-years old and it was still on the police database. In another case, an accountant, who wanted a Green Card to go to America, had stolen his father's car when he was 18-years old. That was still on his record and that could have prevented him getting a Green Card to go into the United States as a chartered accountant. These are examples—and there are many more like this—where even accurate information, let alone the problems with suspicions or untrue information, can cause detriment if it is kept for too long.

Q50 Gwyn Prosser: Those are matters about how long you keep this information stored. In terms of access, let us take a children's library. Some children's libraries use a fingerprint system now. How difficult would it be for the police to have access to that? How serious a crime and what test would they have to pass to be allowed access to that, which could be very sensitive

Mr Smith: At the moment the test is with the school. The police make an access request. The school looks at: "Would we breach the Data Protection Act if we respond to the police?" If they can say that not giving the information would be likely to prejudice prevention or detection of crime and does not say a level of crime, or the apprehension or prosecution of an offender, then they can give that information without breaching the Act. A low level of crime would justify that. The information might be of limited use to them because of the way it is stored. Those fingerprint systems in schools would not necessarily be compatible with the way that the police use fingerprints. But the test is fairly low.

Q51 Gwyn Prosser: Would the school or library have to inform the youngster or the parent?

Mr Smith: They would not have to, although we would recommend as part of good data protection practice that they do notify people, unless doing so would essentially be a tip-off which would harm the police investigation.

Q52 Gwyn Prosser: We have talked about store cards and I would like to ask you about police access to store cards. How reasonable would it be for the police to say, "We want to access a whole series of store cards, because a particular item has been found and we want to see who has had possession of such an item in the recent weeks or months." Would that be far too wide a net to cast?

Mr Smith: The police have accessed store card information in the course of crime investigations. We would expect a supermarket to say to the police: "Look, have you narrowed down what you want? You are asking us to give this information. We have a decision to make. Have you narrowed down sufficiently what you want and is the crime sufficiently serious?" We had an example not so long ago to do with airport workers. There had been an incident and the police asked for details of everybody who was on duty between certain hours.

We basically said, "Where did the crime take place? What was the nature of the crime? Actually you only need this smaller group." But you do need a group. You cannot pin down one individual because you are looking at suspicions. That is the whole approach: narrowing down what you need.

Q53 Gwyn Prosser: Would you consider there would be sufficient narrowing down in a case where the police said, "We want to do a widespread search of store card purchases in order to gauge the lifestyle of particular individuals"?
Mr Smith: I hesitate to say, off the top of my head, "That's going too far" but that is my initial reaction. Are you really seriously going to be able to help detect a serious crime in that area? We would be most concerned where you have no crime and you go and look at the lifestyle information to look for—

Q54 Gwyn Prosser: Fishing.
Mr Smith: Yes, fishing, absolutely.
Mr Thomas: One can see, in the fight against terrorism, that if there had been a purchase of materials to build explosive then one might want to track through all the suppliers of that and see where sales went. But on the more general question, the banks, for example, are very precious about maintaining confidentiality of banking information. I am not sure if people like Nectar are giving evidence to this Committee but they would have strong views to share with you on police and other access to their database which they do safeguard very jealously.

Q55 Chairman: I gather from what you said to Mr Prosser that, in principle, you are quite happy with the threshold of tests that the law applies
Mr Thomas: Indeed. Section 28 national security, section 29 law enforcement. Those are in the statute. We are happy with those.
Chairman: Good. Thank you.

Q56 Mrs Dean: Before I move on to my question, could I ask whether it could be beneficial for the Child Support Agency, on behalf of parents with care of children, to be able to access lifestyle information on people who should be paying to support their children.
Mr Thomas: I am not familiar with whatever legal powers they have. It may be that the Child Support Agency has powers to inspect tax records and work records and bank records. My colleagues may know in more detail than I do but I think we would start with the proposition that a body like that has a job to do but if it is going to obtain information from elsewhere then that must take place in a way which is lawful and fair and then fulfil all the other data protection principles. We deal with a very wide range of bodies and I am afraid I am not familiar with exactly what the powers are. If they can make a good case out and that would be acceptable in fairness terms and they have the legal power, then I would have thought that would not be a problem.
Mr Smith: It is a slightly different point but I think it is worth bearing in mind, Chairman, that you are often faced with conflicting public policy objectives in situations like this. There is clearly a desire to decrease things like benefit fraud—which you might be talking about in the area of the Child Support Agency—but there is also a desire to increase the take-up of benefits by eligible people. The more you ratchet up what you collect from benefit claimants and the more widely you share it, there is a real risk that you will put people off claiming. You see the same in the Health Service. There are some very interesting arguments in the Health Service.
Chairman: I am going to stop you, Mr Smith, because we are going way off the question.

Q57 Mrs Dean: Data protection gives the right to know what information is held about us but we can give up personal information without realising it. You mentioned earlier that work has been done on health-related databases but should we have clearer rights to decide whether our data can be shared, even if in that opting out, for instance, of health-related databases we accept that there are risks in not sharing the data?
Mr Thomas: Again, I think it depends on particular circumstances. We had an exchange earlier about health records. If there were a scenario where you insisted that your information stayed with your GP and was not to be shared under any circumstance with hospitals, then I would certainly expect the risks of that to be spelt out, so you would be told, if that choice were to be available, by exercising that choice you are running a very serious risk that if you are taken by ambulance to the local hospital they will have no information on you. That is a fairly obvious example of spelling out the consequences to people. We talk a lot about choice but I think the general proposition is that any choice has to be an informed choice and that is why we put so much emphasis on transparency and fair processing notices, so that people are told why the information is being collected, how it is going to be used. It does not really matter if 100% do not read it or understand it; the mere discipline of the obligation of the organisation to have to put in writing and to communicate with their customers or their citizens why they are doing it in itself is highly beneficial. This point arose earlier and I think we accepted that many people do not read the small print and do not fully understand it. The mere fact that they have to communicate in itself I would say is a public good.

Q58 Mrs Dean: What effect do you think an increase in penalties from unlawfully obtaining personal data will have?
Mr Thomas: Quite dramatic, I hope, because there is a very pervasive and unacceptable black market out there. There is a network of private investigators. Their clients include banks, insurance companies, newspapers, law firms. For a wide range of reasons this personal information is being obtained from many organisations. For any member of this Committee or any member of the public here I could say what the tariff is for getting your personal

information. I know how much it costs to get into this market because we have seized the materials using our search warrant powers. I could say how much to get your mobile phone records; how much to find out if you have a criminal record or not; how much to get hold of your DVLA records to see who owns the car parked outside your house last night. We documented this very fully in our first ever report to Parliament in May last year. I think that caused quite a lot of surprise. People suspected it was going on but this was the first time it had been properly documented.

Q59 Chairman: Could you remind us what a couple of those prices were.
Mr Thomas: I do not have the report with me, but it ranged from about £75 for the easiest information up to about £750 for the more difficult information. Our report set out the full tariff. To find out who owns the car parked outside your house last night is about £75. These people often work through networks. One agent specialises in British Telecom, one in DWP, one in DVLA. They all interrelate to each other. It is a criminal offence. It has been a criminal offence since 1994. We prosecute cases. They often ended up with derisory penalties: a conditional discharge for one of the most serious ones, or very, very low fines. I am afraid this was a Commissioner who got very angry about this, decided Parliament needed to be told about it and I am delighted that it has been taken seriously. As soon as time is available in Parliament, I hope this Committee and others will support that initiative when it comes forward. It has already been a wake-up call for the private investigators and their users. Already we are seeing better penalties coming through from the courts using their existing powers, but there are quite low thresholds there. It has had quite a dramatic effect on this particular industry but there is a long way to go yet. I have to say that the newspapers are not keen on my proposals. I am being attacked as a threat to freedom of speech, which I thoroughly deny because there is a defence there. If you are doing this in the public interest, then there is a complete defence.

Q60 Mrs Dean: Are your protocols for handling information sufficient to safeguard privacy or should your office have more power to conduct inspections and impose sanctions on negligent or reckless data controllers?
Mr Thomas: I think this is where we move on to our inspection powers. The law says what I can do and what I cannot do and we take our obligations and our powers very seriously. The law at the moment says: "The Commissioner may with the consent of the data controller assess any processing of personal data for the following of good practice and shall inform the data controller of the results of his assessment." The key words there which we find very limiting are "with the consent of the data controller". This was a point I started making earlier. We are a regulatory body. We are unusual because we regulate government and other parts of the public sector. We are not completely unique in that. We certainly regulate the private sector as well. I have been a regulator in other environments. I find it very bizarre, frankly, that we have to have the consent of the organisations we are regulating in order to find out what is happening in practice. This case has been put to the Home Office, the Lord Chancellor's Department, the Department for Constitutional Affairs, the Ministry of Justice. We have been putting this case on a regular basis, where they smile and say, "We will do what we can" but we have not yet had a firm commitment that they will change the law. There is some pressure now from the European Commission to change it as well. I hope this Committee will understand that whatever protocols or codes of practice, data protection principles, whatever people tell us about what they are doing, sometimes it is what is happening in practice that we need to go in and investigate—not necessarily in a threatening way. We often will go in and carry out an audit to help people get it right, but, to know the regulator can step in has a very sharp deterrent and therapeutic effect upon organisations.[1] To know that they can turn me down and say No and my inspectors and my investigators and my auditors cannot go in now, or not until they have put things right in 12 months time, does have an unfortunate effect on the dynamic of us as regulators. We have come to this Committee with one or two specific proposals. We are recycling something we have said to the Government in the past but we hope you understand why we attach weight and importance to it.

Q61 Bob Russell: Mr Thomas, that leads us neatly into the section I have, which is the monitoring of abuses. I picked up on your earlier observation that 86% of the general public regard safeguarding personal information as a major priority. In that context, technology puts employers in a powerful position vis-à-vis employees during the working day. As MPs we are aware of that from our whips' office! Have you detected a rise in the number of cases of abuse of surveillance technologies in recent years?
Mr Thomas: In the workplace, I think it is going down, if anything. We can claim some credit for that. We launched a code of practice with the full support of the TUC and the CBI, with the three bodies together at the same time launching our code of practice. The code was a difficult one to write. We had to rewrite it several times. It covers all aspects of monitoring staff in the workplace. It covers recruitment, personnel records, monitoring email and internet use, health checks. It is a wide-ranging code. David can take enormous credit for being the principal author of that. In its early stages it was the victim of some criticism, of being a bit too lengthy and a bit too detailed. We got it right in the end and we got a lot of praise from many organisations. The human resource/personnel industry now understands that here is the Information Commissioner's code of practice, it is seen as helpful and I do not think we get any serious complaints. I

[1] *Note by witness:* As a regulator, to be able to audit organisations without their prior consent would have a much stronger effect.

am sure we get occasional complaints but we are not getting anything like the volume of complaint one might otherwise have expected. Members of Parliament I do not think are employees, but the principles of the code might apply in your context.

Q62 Bob Russell: That is a fascinating response, bearing in mind we have just started our inquiry A Surveillance Society? I was going to ask what scope is there for the Information Commissioner's office to do more monitoring work in this area and you are telling me that the work you have already done has led to matters being improved. There is less invasion by employers against employees.

Mr Thomas: The risks are still there but I would say quite vigorously that the fact we were able to secure an agreed code of practice—we got agreement and we pushed this very hard around the employer community, and the trade unions have taken it seriously too—shows that in the particular context of the workplace—and data protection creeps everywhere, it is a horizontal law—the risks of excessive surveillance have been very substantially reduced because of our code of practice and I am proud of that. I would like to see the same approach apply in many other areas where surveillance remains a considerable risk.

Q63 Bob Russell: That leads me on to my next question: what steps can be taken to make it easier for organisations to detect abuse of their databases? What incentives could make organisations work harder to protect them?—and organisations can mean anything you can think of: statutory, voluntary or whatever.

Mr Thomas: I am not sure whether your question is gauged more at a new initiative or just keeping the existing system in good order.

Q64 Bob Russell: We have new technology and you have explained very successfully how employers, as a general rule, and the workforce, as a general rule, working together, have reduced that danger of a surveillance society. But the question now is about organisations. I am not going to name the organisations—they could be statutory, they could be voluntary or it could be a members club or whatever—but organisations which have electronic retrieval systems.

Mr Thomas: I think the general message, yet again, is that they must take the legal and the good practice requirements seriously. We have put a lot of guidance out. We have moved away from perhaps a slightly theological approach to data protection, which is rather abstract. Now we have put out a lot of guidance notes, good practice notes—Do this, do that; do not do this, do not do that—in a wide range of areas, so we are getting a good feedback on that. More generally, we have already talked about strengthening our inspection powers. We would like to see a penalty associated with legislation. At the moment our only real stick is an enforcement notice which says "Do not do it again". There was an example last week of the Health Service recruiting doctors. I am sure many Members of the Committee read that the Department of Health website was shown to be insecure. People could see all their colleagues' application forms and details of their criminal records, their health history and all the rest of it. The Department of Health was obviously quite in the wrong. It was wholly unacceptable. It put its hands up and their website was closed down within half an hour. I do not give them praise for how they got there; I do give them praise for closing it down within half an hour. There is not very much we can do in that situation. I do not think they will do it again in a hurry; certainly, therefore, an enforcement notice on the Department of Health would have been not very meaningful. We are exploring and we would like this Committee to explore the idea that for situations where there is a flagrant or a negligent or repeated disregard of the requirements of the law there should be some sort of penalty. This is not rocket science. It is the norm in other areas of regulatory life and we think it would serve as a very useful tool to concentrate minds to prevent the sort of problems you are talking about. I do not want to prosecute left, right and centre, but I would like there to be a deterrent and, in the extreme case, where there had been unacceptable disregard of the regulations, to be able to go to court and have a system of fines to sanction that behaviour.

Q65 Bob Russell: You have made a powerful case there that there should be penalties for the abuse of surveillance technologies. Would you be prepared with your colleagues to consider submitting to us a suggested tariff as to what you may have in mind so that we can consider that? Do the ICO or other agencies have sufficient investigative powers in this respect?

Mr Thomas: On the first point, of course the answer is yes. We floated the idea in our submission to you. If the Committee would like us to elaborate on any other point, we will elaborate with a written submission as to what a scheme might look like in terms of how you might define the offence and what the associated penalties would be. Mr Russell, we have probably answered your second question on our investigatory powers.

Mr Smith: There is an example which relates back to your question about employment monitoring and to this question of offences or possible offences. We have had a case where essentially a secret camera was installed in a workplace, caught an employee vandalising a machine and the employee was dismissed as a result of it. The secret camera, because it was secret, was in breach of the Data Protection Act. The employee was dismissed and appealed to a tribunal. The tribunal, perhaps quite rightly, said, "Well, we can't ignore the evidence. However it was obtained, you did something wrong," the dismissal was upheld, but nevertheless you are left with that employer who had essentially breached the Data Protection Act in obtaining the information. The only power we have is to issue them with an order to say: Do not do it again in the future, but that is a set of circumstances where that problem will not arise again. There is no sanction for a breach of the Act.

It is that that we are looking for: knowingly and recklessly breaching the Act in a way that causes harm.

Q66 Gwyn Prosser: You have painted for us a very worrying picture about the trading of illegal identification and personal information. I sit on the all-party identity fraud group and we have been told there is something called the "deep web". This is an internet system which is closed to the rest of us on which there are thousands of transactions going on every day apparently: offers of identity, offers of information which you could put together and then steal someone's identity. It is all very worrying. It fits in with the pernicious black market you were talking about. Could you tell us about your experience of the impact of being the victim of identity theft or of the supply of personal information about an individual? Perhaps you could give us some hard cases or one hard case on the individual.
Mr Thomas: First and foremost, when people find their identity has been stolen there can be severe financial consequences. Even if the banks and others assume some ultimate liability there can be a horrendous amount of hassle and worry for people to sort matters out. When people suffer financial loss, even if it is reimbursed, there are real negatives there as a result of identity theft. If people find they are being impersonated their reputations can suffer. It can be in the workplace, it can be in their social environment, with their families, all that sort of area. Moving into a different sort of set of examples, if people's private lives are unjustifiably intruded upon, there can be a very, very, real deep sense of outrage. If people think that what they are doing in their private lives is suddenly available not even to the tabloids and the newspapers but to other organisations, then they find that wholly unacceptable. In one of the examples we had, a man was suspected by an insurance company of making a bogus insurance claim—a genuine claim, as it turned out, but they thought he was making a false claim and they are entitled to make legitimate investigations. The insurance company hired one of these very dubious private investigators. Within a very short time indeed, they had telephoned his 82-year old mother, pretended they were from the Inland Revenue, obtained details of her maiden name and other personal information. We have these conversations on tape, by the way. Within 10 minutes of getting that information from the mother they had gone to the bank account in order to find out more information about how that individual conducted his financial affairs. You may say he suffered no financial loss—he might have done, he might have been turned down for his insurance claim wrongly, but in fact in that case he suffered no financial loss—but when he found out what had happened he was absolutely outraged. We have a large number of examples like that in our report, Mr Prosser. I could go on but that gives you a flavour of some of the activities. I have to say it happens in the political arena too. You may say politicians are public figures, they are fair game, and I will not comment on that, but there were secretaries of politicians who were having their personal lives invaded in this way, which I think is absolutely outrageous, and I am very glad we are going to see legislation on that particular point fairly soon. I think it does illustrate the wider issue about some of the risks of surveillance. If you collect information, the risk of it being improperly accessed must by definition increase.

Q67 Gwyn Prosser: On that issue of improperly accessing this information, do you think some of the organisations that store the information tend to be a little bit complacent about the safeguards?
Mr Thomas: Yes.

Q68 Gwyn Prosser: Would it be helpful if they had more liaison and more connection with the work you are doing?
Mr Thomas: Yes. I think there is a lot of complacency and a lot of people are very shocked when we reveal to them how their systems can be so easily breached. We work very closely with bodies like the DWP, British Telecom. We have arrangements in place. If they have suspicions, they come to us. My investigators are mostly ex-policemen and we go out and investigate. We have search warrant powers. We do cooperate, particularly with organisations with call centres because the telephone call centre can be a particularly vulnerable weak point, but there are other ways in which people are really quite shocked to find out how easily their systems have been breached. We do what we can but I think there is a lot of self-interest at work here because organisations do not want their security breached and they are working very hard themselves to prevent these problems.

Q69 Mr Clappison: Could I come on to the subject which we touched on a moment ago: mandatory privacy impact assessments. What do you see as the prospects for the introduction of them into the UK and do you think they will be practical in terms of keeping pace with technology developments?
Mr Thomas: Could I break it down into two sections, first of all, just to share with the Committee what we mean by privacy impact assessments and then discuss whether it should be mandatory or not. My colleagues will amplify my remarks, I am sure. It is a methodology which is quite widely used in other parts of the world which is still not familiar in this country. We are looking at something entirely new. Essentially a privacy impact assessment is an attempt by the organisation which is going to be collecting information in new or enlarged ways to record what they are going to do, why they are going to do it, how they are going to do it, to identify the various risks associated and to spell out publicly how they are going to mitigate those various risks. It is a discipline. It is a sort of risk management or risk assessment programme. It has caught on in other parts of the world. In the United States now it has been mandatory under the E.Government Act of 2002. I have here, and I would be happy to send a copy, "The privacy impact assessment"—the official

guidance from the Department of Homeland Security. In the United States this is mandatory but they embrace this approach with a very constructive positive spirit and it seems to be beneficial. Here is the DHS charged with safeguarding the security of the American people. They are taking it seriously. We have talked to a number of government departments and they all say "It sounds a good idea, but we are not really quite sure what it would involve". There is no hostility to the idea. Later this year we are going to be producing a great deal more guidance for a UK environment as to how it might work and what the benefits would be. We are expecting a fairly warm reception to what they have to say. I think people do genuinely want to find out how it would work. We all want to avoid unnecessary bureaucracy. We are keen to spell out this will not be a bureaucratic intervention. The second part is whether it should be mandatory. My answer is that if public sector bodies, particularly central government, refuse or are reluctant to go down this road, then I think the case for a mandatory requirement to carry out a privacy assessment becomes very much stronger. It will only work if it is done in a positive spirit and you explore that first.

Q70 Mr Clappison: You mentioned in the first part of your answer that you would be coming back later this year to the question of the benefits. I wonder if you could give us a foretaste of that. How would you spell out the benefits of this to the public in straightforward terms?

Mr Thomas: I cannot do very much better than read out what the Department of Homeland Security say. They say: "This PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. The purpose is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire lifestyle of the system. It is built into a system from the start. Addressing privacy issues publicly through this PIA will build citizen trust in the operations of the Department of Homeland Security." I will not read more but it goes on to spell out what they are doing and how they expect to reinforce that trust and confidence and reassure the public. There are a lot of anxieties. The Chairman's very first question was: Are we being paranoid?—if I may paraphrase your first question. We do not think we are, but we do think the public need reassurance and we believe this is one way in which reassurance can be given.

Q71 Mr Clappison: You are saying to us that this fits in with the work of your office.

Mr Thomas: Indeed. We have not done much in the past but we have started this debate over the last six months or so and we see this as a real, attractive opportunity to push this case. Jonathan is overseeing the consultancy we now have in place to bring to the surface clearer ideas as to how this methodology would apply in the UK environment.

Mr Bamford: Within the next month or so we are going to put out an invitation to tender for people to draw up privacy assessment methodology and also a handbook. The New Zealand Privacy Commission has developed a handbook. If we are bandying definitions around, it is interesting to add one point in their definition which I think is relevant when we talk about a surveillance society and things like that. It says in here: "A privacy impact assessment will sometimes go beyond an assessment of the system and consider critical downstream effects on people who are affected in some way by the proposal". It is not just looking at what is the safeguard there, it is looking at what the consequences are for the individuals affected and then modifying the system to take account of those. We are very keen to make sure we have something that works in the UK environment. To answer the second point of your question as well, to what extent PIAs are technology proof because of changes in technology, I think I would go back to what I said about the data protection principles being largely robust and technology proof. A privacy impact assessment will be rooted on the data protection principles, so questions about the integrity of the data, its accuracy, the security, what people are told, those are timeless questions that are not dependent upon technology. They are relevant questions all the time, so I think the privacy impact assessment will live beyond just the point of publication.

Mr Thomas: Our written evidence to you records—it is very welcome—that the Department of Transport has offered to work with our contractor to allow its plans for road charging to be used to provide a practical basis for where we are coming forward. They are exploring road charging. It is a controversial area. Privacy is one of the issues in that and I think it is a very welcome gesture from the Department of Transport to cooperate with us to explore this methodology in the context of road charging.

Q72 Chairman: It is interesting that that document has come from the Department of Homeland Security, which implies that the US authorities are planning to apply this to areas of terrorism, serious crime and so on. We also know that the same US authorities have obtained the credit card details of millions of European citizens through targeting the Belgian organisation which handles all this information with demands for a vast amount of information on all of us before we try to fly to the United States of America. Have you any sense that these privacy impact assessments are having any effect at all on the way the US Government is going about its business?

Mr Thomas: Again, Chairman, you touch on the competing public interests. We all want to tackle terrorism. We all want to safeguard our privacy. You mentioned the financial data available to the Americans and we also have a debate about airline passenger information, but it is my impression—I do not have empirical evidence—that the Americans are struggling with exactly the same issues we all struggle with. They do not have a data protection

framework but, in the last four years that I have been in office, privacy and safeguarding the individual have shot up the congressional and public agenda in the United States quite dramatically. I went to one conference in Washington three years ago and there were about 400 people; I went this February and there were 1200 people. It was front-page news right across Washington. People are very concerned indeed about the state having either too much information or abusing their information. Equally, the government turns round and says that we need to identify those who present a risk to society. I think there is stronger experience in Australia. Jonathan mentioned New Zealand, Canada, where this methodology has been in place. Our impression—and I would not go beyond impression—is that it really has had a beneficial effect on getting organisations to take the issues seriously, and, above all, to address them at the architecture design and not as a bolt-on later in life when things start going wrong. It is a great deal more expensive that way round.

Q73 Mr Winnick: Perhaps we could get a copy of that booklet.
Mr Thomas: We have a lot of material to give to the Committee, Chairman.

Q74 Ms Buck: Could I ask you to tell us about the pros and cons of privacy enhancing technologies.
Mr Bamford: The whole idea behind privacy enhancing technologies is a way of using the technology itself to help protect people's privacy. We know how technology can do all sorts of wonderful things for us but let us use it in a way where we can deploy it to protect individuals' privacy in some way. Whether that is limiting the amount of information that is collected about individuals or perhaps using more sophisticated identity management techniques, but thinking about a way of using the engineering itself to look after individuals in some way. This is something which within the data protection community internationally has gained a lot of leverage, really to try to make sure that technologists do try to design privacy in. One of the slightly more frustrating aspects of our role in many ways is particularly when government departments let contracts for major IT systems have moved more to say, "Well, you deliver what we want and we will give you a general overview" but they do not specify, "And we want you to do that in the most privacy friendly way" so the contractors never bother to try to come up with a more privacy friendly way. A concept of saying how can we do things here that is more privacy friendly is quite welcome. Interestingly, the Royal Academy of Engineering, which has just published a report, has very much latched on to the idea of privacy enhancing technology. These are the technology people who are speaking and they recognise there is a way of using technology to enhancing privacy, so we are quite supportive of the idea. Again, as the Commissioner says, it is something which you cannot think of as an afterthought really. It is something that is built into the system. We have talked about our issues here about information sharing for transformational government. In Austria their e.Government approach is essentially to try to dispense with a central identification number for all the Austrian citizens to tie together government services. I will not go into the technology because I cannot say that I really explain it myself that well but, basically, it means you can use different ID numbers for different services but the systems recognise the ID numbers without having to exchange and keep all the ID numbers. You can see how, if you do not have one powerful ID number, the collateral risk to the individuals of tying together information is reduced to only certain aspects. The Austrians have managed to do some interesting work in this area and it is somewhere that we would encourage government departments and the major private sector organisations to think about. Identity management is one aspect there and we are trying to sponsoring some more work in that area such as the Oxford Internet Institute which is having a symposium on identity management to see if there is a way of dealing with identity that does not involve really large collections of information all verifying that I am the right Jonathan Bamford, with my driver's licence number, passport number being replicated in lots of different databases.

Q75 Ms Buck: You sound quite enthusiastic about it. The criticism is the extent to which it is a technological fix for what is not fundamentally a technological problem. But that is not the implication you are giving. You see it as quite integral if it is done properly.
Mr Bamford: The way I like to think of it is as one of a number of measures that help. I do not think you can simply say there is a killer answer, the silver bullet solution, but it must be right, must it not, if we think there is a risk out there of big collections of information falling into the wrong hands, being used in ways that prejudice individuals—perhaps it is Mr Prosser's example of identity theft which is clearly facilitated through that—we must try at the outset to stop that information being misused in that way through technology helping prevent that misuse. That does not mean to say there are not other procedural safeguards, legislative scrutiny safeguards which would also go there. I see really it is more of a jigsaw of things that fit together and I would not like that piece of the jigsaw to be missing really.

Q76 Chairman: The more the databases grow, the more we can do profiling. I suppose that is what credit risk agencies do. Effectively, they build up a profile of people's financial records. As the potential to profile individuals grows, would you like the Committee to be saying that we restrict the ability or the circumstances in which you could do profiles or simply to raise awareness of the fact that profiling can take place?
Mr Thomas: I think raising awareness is the priority. You quite rightly said that profiling has now become very sophisticated in the private sector. People know

what sort of books you are likely to read. They know what holidays you are likely to be interested in. That has become a very sophisticated technique. The same techniques are now being explored and to some extent deployed in the public sector. But it is a bit like children at Christmas: there is a risk that people think we can do anything now through profiling, and I think we would like this Committee to sound a very grave warning about some of the risks. If you get it wrong, particularly in the public sector, you can get it very badly wrong. In the report we commissioned this is discussed at length and some of the risks are set out. I hope the Committee will look at those. They talk about profiling and also social sorting where the computer gathers information about you, it labels you and characterises you. Let me give you a few simple examples. At one level, if at one time you are dealing with social services and they write down "heroin addict" that might have been true 10 years ago, is it true now? Is that label around your neck for the rest of your life? If you then start putting snippets of information about you together—where you live, your postcode, whether you have a phone, the criminality patterns of your parents—you can build up images of people which may take you in the wrong direction. If you are trying to identify children who will commit crimes later in life—the Cabinet Office is doing a lot in this sort of area—I understand their motivations and I understand what they are trying to achieve, but if they get it wrong—if they label that youngster as someone who is going to be a criminal in 10 or 15 or 20 years time or that family as a problem family—it needs our intervention. Technology can take you a long way but it is not going to be 100% effective. When we raised concerns about profiling, we raised concerns about social sorting. It is to signal the risks involved without the human intervention. Machines can do a lot to gather and to help you inform your decisions but without the human intervention I think there are grave dangers. My answer to your question, Chairman, is that absolutely paramount is the importance of raising awareness as to the risks involved. I do not come to you saying there should be a ban on profiling by the public sector. We are not suggesting that. However, as with so many things, I say proceed with caution, amber light in this area, because if public bodies embrace the potential of the technology too literally and too enthusiastically it will undoubtedly create the sort of climate of suspicion, lack of trust and real problems. It will only take a handful of star examples which get splashed over the newspapers to destroy all the good work that the health authority, the social services, the education and all the other people are trying to do to use information intelligently.

Q77 Chairman: Given the risks—and of course we saw them in the private sector perhaps a lot more two years ago than we do now, with credit reference agencies and people being wrongly denied credit because of wrong information and so on—is there a case for having some formal government procedure that ensures that, if profiling is going to be done, those who are going to use it have properly assessed its potential liability, what it can tell you, what it cannot tell you and how the possible risks should be handled? Should that be made a formal part of legislation or should it linked with the privacy impact assessments or with something built into the UK Government?

Mr Thomas: It goes back to the debate about whether PIA should be mandatory or just done because it is good practice. I am happy to start with the good practice route and I would see the suggestion you are making as an excellent suggestion to fit within the framework of a PIA. If a particular system is to use profiling techniques, then a section of the privacy impact assessment would spell out what is going to happen, how it is going to happen and how the various risks are going to be addressed. And then we would like to have our inspection powers to make sure it happens in practice. Could I link that to one suggestion I would like to share with the Committee this morning, Chairman. It was not in our written evidence but we do have the power under the existing law to do a special report to Parliament. The report on *What Price Privacy* was the first time we had used that. If the Committee were so interested, we could think in terms of an annual surveillance report using our special powers to record what developments there had been over the previous 12 months, the extent of our involvement, what we felt we had achieved in terms of promoting good practice and areas where we had some concerns. If we could do that in a way which rooted into our data protection responsibilities—we could not address all the issues—but that might be a suggestion the Committee might like to think about.

Chairman: It is certainly a very interesting suggestion and one I am sure we will bear in mind as we go through the inquiry and come to our report. That takes us neatly, I think, to the last question.

Q78 Mrs Dean: Thank you, Chairman. Given the pace of technological development and the drive by government to share and use information to deliver public services and fight crime, in which particular areas should developing ground rules be the priority?

Mr Thomas: I am going to ask David to say a bit about the importance of educating the public because that is a very important priority as well, to make sure the public are educated. We have done some work and he will say more about that. As a broad proposition I would say the public sector needs to have priority at the moment over the private sector. It goes back to the exchanges we had earlier, because I think there are commercial and other pressures impacting on the private sector which I see being taken very seriously indeed. The state has a monopolistic and often a mandatory power over citizens and it can do things without their consent, without their agreement, without their involvement for perfectly good reasons. The state has, if you like, greater potential but also can cause greater harm if people are wrongly labelled, if they are wrongly identified, if mistakes are made. Also the state tends

to have larger numbers. The databases run by the state are much, much larger, so if things go wrong within a public sector database the effects would be multiplied many times more. We talked about the doctors' database going wrong last week. Several people made the point that it was only a handful of doctors compared to the millions and millions of patients on that single spine for the National Health Service. If something went wrong and everyone could see your health records.—well, that would be catastrophic. If I am asked to select areas, I would say public sector against private sector. I would then say, broadly speaking, in the Home Office area which this Committee is particularly shadowing. I know I have gone wider than your immediate responsibility but I do think the Home Office, the Department of Justice, the Ministry of Justice sort of area is the area where there is the most difficult challenge because there, for understandable reasons, people are collecting and using information. But that is where there are the most coercive powers against the citizen, and that is where, unpopular though sometimes it may be—and after yesterday's trial I know this is difficult territory—sometimes the importance of upholding liberties means that an independent commissioner has to say things which may be unpopular in the short term. But by putting weight on those areas I am not minimising taxes, criminal records bureaux, social security. We have a long agenda.

Q79 Mr Winnick: Back to 1984.

Mr Thomas: I am happy to live in 2007, Mr Winnick. Could we say a word about education.

Mr Smith: It is probably right, Chairman, just at the end to go back. You asked us about our vision earlier on and part of that vision was an aware population who know their rights and are confident in using them. That is one of the protections against the excesses of the surveillance society. We have not concentrated much on it today. I think it is right to bring it in at the end and say that we do see it very much as our part of our role to bring about that education. We have produced things like a personal information toolkit earlier this year which advises people how to protect themselves against identity theft and it advises them how to access their information. I would like to put that firmly on the table: it is about educating and encouraging people to use their own rights as much as about what we can do as the regulator.

Chairman: Thank you, Mr Thomas and colleagues. You have got the inquiry off to a very good start this morning.

Thursday 7 June 2007

Members present

Mr John Denham, in the Chair

Mr Richard Benyon	Mrs Janet Dean
Mr Jeremy Browne	Gwyn Prosser
Mr James Clappison	Martin Salter
Mrs Ann Cryer	Mr David Winnick

Witnesses: **Mr John Trevor Hughes**, Executive Director, and **Mr Randal Gainer**, International Association of Privacy Professionals (IAPP), gave evidence.

Q80 Chairman: Thank you very much for coming before us this morning. You have been told that this is one of a number of hearings to explore the suggestion by our own Information Commissioner that we are moving towards a surveillance society and, if true, what the implications are and how government should respond to that. We are particularly grateful to both of you for coming because we know that you have taken time out of a visit to London to do with your work as privacy professionals. Perhaps for the record you would start by introducing yourselves.
Mr Hughes: My name is John Trevor Hughes, Executive Director of the International Association of Privacy Professionals based in York, Maine, in the United States.
Mr Gainer: I am Randal Gainer, an Attorney based in Seattle with the law firm of Davis Wright Tremaine.

Q81 Chairman: Thank you very much for coming and for your evidence. I begin by asking in particular about private sector companies with whom you work. Does the work that you and your members do go beyond trying to help companies not to be caught out by regulators?
Mr Hughes: The very short answer is yes. Let me start by describing the profession of privacy and the people we represent. The IAPP is a professional association representing people who work in the field of privacy. We have almost 4,000 members in 23 countries around the world and do all the things that a professional association would normally do for its members. We educate them, provide opportunities for them to meet and share ideas and also certify them so they can show a credential to the marketplace and be able to demonstrate their skills and knowledge. Over the past 10 years we have seen a migration within the profession of privacy. When I started as a privacy professional I focused on compliance. As an attorney I focused on keeping companies out of trouble, but that is perhaps an older and more antiquated way to approach data protection and privacy issues within corporations today. We find that our members are talking more about trust and engaging consumers in a meaningful dialogue to engender trust. That goes beyond compliance and legislation and regulatory requirements and speaks to a business imperative to create a more meaningful relationship with customers. That is the long answer to your question. We find that these days most definitely companies move far beyond mere compliance to try to attain a higher and better relationship with their customers.

Q82 Chairman: I am sure that is an accurate reflection of the concerns of your members as professionals. Is it universally accepted by the organisations for whom they work that this goes beyond compliance?
Mr Hughes: That is a good question, and certainly privacy professionals are the converted. We believe in the field in which we work and that varies by degree depending on the company. It would be inappropriate to think of privacy professionals as limiting information flows. We find that privacy professionals to varying degrees of sophistication within different organisations try to help maximise the permissible or balanced use of data within an organisation to maximise the value that can be gained from it. It is certainly true that if we want the information economy to grow and flow its currency is data. Data must flow in order to create value. Many of our members and to varying degrees the companies for whom they work focus on maximising the permissible and valuable use of that data.

Q83 Chairman: In your organisation are there as many public sector professionals as private sector professionals?
Mr Hughes: It is not an even split. We have a good number—I would have to check but it is many hundreds—of governmental professionals. We offer certification for the governmental sector. It is notable that in the United States there are requirements placed on government that all federal agencies appoint a privacy liaison. That has led to the appointment of chief privacy officers within most if not all federal agencies. These are distinct from, say, a privacy or information commissioner as may be found in the UK or Europe. They are not regulators but privacy professionals who advise on data protection and its use within an agency.

Q84 Chairman: Is there a difference in the culture of those members? As is always said, we are two nations divided by a common language. The word "privacy" in the way it is used here is often assumed to mean the restriction of the use of data. You have made it very clear that you are talking about properly handled flows of information. Do you find

that the public sector professionals have that same understanding of what privacy is about professionally, or do they have a different view because they are in the public sector?

Mr Hughes: I think that public and private sector professionals approach issues differently. Certainly, the issues are different. In the private marketplace professionals are trying to help organisations maximise the permissible use of data so as to create value for their organisations. They do that in ways that are certainly compliant but hopefully also in ways that engender consumer trust so as to engage in a long-term relationship with customers. It is somewhat different in governmental sectors. We do not take positions on these matters, but I certainly hear from our governmental members that they feel perhaps a stronger commitment to protecting citizens and dealing with concerns associated with terrorism or fraud. That certainly changes the approach of some privacy professionals within the public sector.

Q85 Chairman: You have talked about the different legislative requirements in the States. Does that mean that perhaps you have rather fewer public sector professionals in your organisation from this country than you would in the USA?

Mr Hughes: That is certainly the case. We are a global organisation with members around the world but most of our members come from the United States. I would have to check, but I am not sure whether we have any public sector members in the UK.

Q86 Chairman: Let me put a big question but I would be happy with a brief response. In your work you see the culture of discussion about these issues in quite a number of different countries. Where would you say this country was in terms of those countries which are most concerned about these issues and those that have least public debate or concern about them?

Mr Hughes: I should state that the IAPP does not take advocacy positions on privacy issues. I am happy to share with you my personal opinion. Just recently I happened to speak to Richard Thomas, the Information Commissioner. We both remarked on the contrast between a European or even UK approach to data protection and privacy issues and the US approach. One of the remarkable things we noted was that in the UK there seemed to be a greater acceptance of governmental use of data. Certainly, in terms of CCTV surveillance there is a greater willingness to allow those things to become part of communities. Just this week I saw an article about a survey in Norway which suggested that over 70% of citizens were very comfortable with more surveillance being put in their towns. I do not think that is the case in the United States. In the US I think there is greater concern associated with governmental use of data. But the inverse is also true when looking at the public and private sectors. In the private sector in the UK there is concern associated with the commercial use of data; there are concerns about discrimination in insurance underwriting, finance, housing and many different areas. In the United States there is a more sanguine attitude towards the commercial use of data and an acceptance that perhaps if data is misused in the commercial marketplace there are some negative consequences, for example discrimination in certain financial products and things like that, but by and large the damage that can occur is another piece of direct mail marketing which arrives in the mailbox. If data is misused on the government side in the public sector the consequences can be quite severe; one can be arrested. In view of the flip of very strong public concern but less concern in the private market in the US—again, this is just my opinion—the fact that the inverse occurs in the UK is quite remarkable.

Mr Gainer: First, thank you for the opportunity to appear here today. Chairman, you asked about the differences between our countries. One is the regulatory approached typified by the Information Commissioner versus a more litigious approach to these issues in the United States. That has produced a very remarkable focus in government on these issues that is illustrated by the report, to which I believe this Committee is responding. I thought that was a very good report which raised a number of important issues. There is no counterpart to that report of which I am aware in the United States. That is a very good thing and will perhaps help resolve some of the issues that have not been resolved in the United States. The other matter is the approach to these same issues through the work that I do in representing clients who have had data stolen from them and are then sued. They have to defend what they have and have not done in that context. I believe that that is a stark difference from the regulatory approach taken here. We can debate which is more effective, but it is certainly a difference.

Q87 Martin Salter: I was interested in your juxtaposition of public attitudes in Europe, particularly Norway, and the United States about data held by the private and the public sectors. Has the passing of the Patriot Act, which is a fairly severe piece of legislation, skewed or had an impact upon perceptions or concerns about what government could do with data, because it worries the hell out of me?

Mr Hughes: We could probably spend a few hours talking about that. In the United States the debate about the balance between civil liberties and the pursuit of terrorists occurred within 24 hours of 9/11. That discussion had already started in the news with politicians, and I think the Patriot Act was a very strong response. Just recently we have seen a retrenchment from the Patriot Act. It is ironic and coincidental that Attorney General Alberto Gonzales was a keynote speaker at our conference in March which had 1,200 attendees, all of whom were privacy professionals. That happened to be the day that the Inspector General's report came out and documented how the Attorney General's office and the FBI had been misusing National Security Letters

(NSLs) basically in the form of a subpoena/warrant-free mechanism to gather data from the private sector. That has created great consternation in the marketplace. I think there was a very strong response to the Patriot Act and a bit of a pull-back as some of those tools are considered by the marketplace to be too strong.

Mr Gainer: It has also affected some of my clients who have international data and are reluctant to have data resident in the United States because they feel it may be accessed inappropriately through those NSLs. It has affected some commerce. For example, I have clients in Canada who have decided not to continue US operations for fear that the data on Canadian residents will be misused.

Chairman: On Tuesday of this week we published a report on European Union issues. It referred in passing to issues to do with the sharing of passenger record data and European banking data with the US authorities. We have made a contribution to that debate in the past few days.

Q88 Mrs Dean: In which countries do individuals have most control over how their personal information is used and for how long it is kept?

Mr Hughes: That is a very good question and I think it speaks to the different approaches that various countries have taken. Certainly, we can look to the European Union and the Data Protection Directive and all of the implementing laws that have been introduced in Member States. We can say that there is certainly a lot of law in Europe on data protection issues. One may argue that that equals a significant amount of control for consumers. It is also possible to look at market forces and say that there have been very positive developments not really in any country but around the world through the web. Many of the tools that we have available today online give us great power to manage through our internet browser how data goes back and forth. There are cultural differences country by country which result in different approaches and different responses. It may be difficult to say who has the most. Possibly one interesting question that we can answer is: are consumer expectations, sensitive to cultural norms and societal demands, in those countries being met?

Q89 Mrs Dean: Are you able to say who has the worst protection of data?

Mr Hughes: You cannot plead the fifth in the UK.

Q90 Mrs Dean: I will move on. Are breaches of privacy through accident or disclosure of personal data less common where regulators have strong powers to inspect and audit systems to protect information?

Mr Hughes: I hope I am responsive to your question. I answer by describing the notice of security breach standards in the United States because I think it is a very interesting comparative law analysis in which we could engage. In California three or four years ago a very simple state law was passed; it was a page and a half, or not much longer than that, which said basically that if in respect of any unencrypted database in which certain data elements were being held you knew or suspected that any unauthorised access had occurred you had to provide notice to all of the data subjects within it that such breach had occurred. Since that time we have seen over 30 states pass very similar laws, some going beyond the California law originally passed, to offer free creditor monitoring services or other mechanisms to help protect consumers after the fact. These are very small laws; they are not very lengthy or big in scope; they do not provide a regulatory structure and it is not really a compliance-driven law but a disincentive to have sloppy data protection practices, because if your database is breached you do not have to go to a regulator or necessarily have to pay a fine, although that exists in some states; you have to go to your customers. For most organisations in the private sector that is a far more painful proposition. Certainly, in terms of the growth of the IAPP we have found that notice of security breach has led to the hiring of many privacy professionals. One can only expect and hope that dedicated people focused on issues of data protection and privacy within an organisation will do something while they are there and it will be for the good of data protection within those organisations. We have seen budgets expand and a growth in concern over data protection. I think that a strong legislative move like that has had a very effective response in the marketplace.

Mr Gainer: In our meetings with German and French officials we asked them if they were aware of the extent of such accidental disclosures in their country. Typically, they were not. I think that is because they do not have a data breach notice requirement in those countries or here, although I understand that EU commissioners are considering the adoption of one. I think that it is an effective mechanism to motivate some companies to do more than they have in the past, but, as I mentioned in my written testimony, I do not think it is sufficient because it is very expensive to deploy adequate security both for electronic and paper records. The fear of disclosure pursuant to a data breach law has caused some businesses to do some work but in my experience it has not been enough. More needs to be done and new laws are being considered in the United States that would encourage businesses to do even more. Those models may be some that you would like to consider.

Q91 Mrs Dean: In terms of the powers, how wide is the variation between regulatory schemes in those countries in which the IAPP has members or contracts? Do you see a variation of those powers in those countries where you have members?

Mr Hughes: In terms of regulatory powers?

Q92 Mrs Dean: Yes.

Mr Hughes: Certainly, we see a broad range of regulatory approaches. As an example, in the United States there is no data protection commissioner. We have many federal agencies that deal with privacy from many different perspectives. The Federal Trade Commission (FTC) is very active in enforcement activity. Close to weekly, if not a couple of times a month, we see an enforcement action

emerging from the FTC on identity theft, spam and privacy protection itself. They have been very active in guiding the marketplace by making a very strong example of bad practices in the market place. But that is not all. We also have health and human services that looks after our major healthcare privacy law. There is a whole host of financial organisations and agencies—the Securities and Exchange Commission (SEC), Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency—that look after financial privacy law. There are a number of agencies all of which have varying degrees of enforcement power. We work and live in an enforcement and compliance culture in the United States. By contrast, in Canada Privacy Commissioner Jennifer Stoddart has the ability to engage in inquiries, but I do not believe that she has the ability to assess fines or enforce. She can refer cases to the public prosecutor but does not have the ability independently to enforce Canada's privacy law (PIPEDA). Between those extremes we see varying degrees of ability to enforce and ability to inquire. We were with our French colleagues in Paris yesterday to hear from the French data protection agency CNIL. The staff of CNIL expressed frustration that they had to ask permission of a data controller of a company before they were allowed to come in, review databases and make sure the practices were in place. There is a great degree of variation as to how those enforcement abilities are documented and provided.

Q93 Mrs Dean: We frequently hear about how personal information is disclosed when computers or disks containing data are lost or stolen. What does this tell us about attitudes towards personal information?
Mr Hughes: The first thing we need to note is that the loss of a disk is not necessarily an identity theft. Disks and laptops are lost and stolen every single day. Today there is a great deal of concern with flash drives that can take an entire database of a million-plus names on a device smaller than a keychain. I think we need to recognise that there is a distinction between loss of data or a device containing data and harm. That said, it exposes that data to greater risk of harm if it is lost. Things like the notice of security breach requirements in the United States change our attitudes towards personal data, as my colleague described; it is changing behaviour in corporate America. I can testify to that merely on the basis of the amount of educational content and programming that we now offer our members on securing databases, training employees so they know how to do the right thing and the number of people we certify. It is certainly changing behaviour.
Mr Gainer: I do not believe that it has changed it enough. In the United States about 10% of lost and stolen data is reportedly used for fraud. In the last reporting period 10% of 73 million Americans were told there had been a data breach. Therefore, 8.3 million had some sort of fraud on their accounts. There is still a lot of work to be done and as a policy matter new approaches must be considered to encourage those who hold data to do more to secure it.

Q94 Chairman: Recently we had a case where one bank sent 60,000 customers' names on a disk through the ordinary post. Does that sort of thing still happen in the States?
Mr Gainer: No, it would not. At times there are losses by bonded carriers, but I have no clients who would make the mistake of sending that kind of protected data through the open mail.
Mr Hughes: I would draw the distinction that large, sophisticated organisations are not making those mistakes, but we always need to remember that small and medium size enterprises are perhaps not as engaged in these discussions and dialogues. I would not be surprised to hear that a small regional bank or operation of some sort was sending a disk through the mail.

Q95 Martin Salter: Of the security breaches that arise, what proportion are deliberate, targeted and criminal activity and what is just straightforward corporate or public negligence?
Mr Gainer: In my experience most are criminal actions. Typically, it is the smash and grab of laptops out of cars, or even desktop computers from office buildings. Sometimes it is electronic penetration of wireless, or even wired, networks among large organisations. There are other times when people just lose disks or other back-up tapes and so forth.

Q96 Martin Salter: Or send it in the post like one of our banks?
Mr Gainer: Exactly. It is perhaps negligence. But the people I have counselled are responding basically to thieves who target either the hardware or data itself.
Mr Hughes: I do not think that for the most part the laptop thefts that we see are one of the key sources of security breaches. They are not really focusing on the data; they want the laptop. Whilst it is a crime it is not necessarily one associated with the data. In the United States we have had two major cases in the past few years related to sophisticated social engineering exploits where people have got in and gathered data. I think that in the case of both ChoicePoint and TJ Maxx—I understand that it has a different name in the UK but it is also a US company—criminals managed to infiltrate their systems, one through just a human exploit, saying they were people they were not and getting data, the other by sitting in a parking lot and catching wireless data on a device as it was going from store to store. In those cases the intent was harm; it was identity theft. They were trying to get credit card data in order to run up charges, but those are two of probably a few hundred notices of security breaches that we have seen in the past couple of years.

Q97 Martin Salter: We have had recent reports of criminal gangs infiltrating call centres to access data. What protection do you have in the United States to stop that kind of activity?

Mr Gainer: Of course there are criminal laws and when those people are caught they are prosecuted and sentenced, but to prevent that kind of intrusion you need a well thought through and implemented security organisation. It has to be tested, revised and upgraded constantly. It is a challenge that many organisations are just now signing up for and have not yet mastered.

Q98 Martin Salter: Is it fair to say that there is an inherent risk of out-sourcing call centres to countries in the developing world in order to cut labour costs, because one could end up with considerably less sophisticated systems of protection to guard against that level of infiltration?
Mr Gainer: There is a requirement in the United States that if those industries that are regulated, because they are financial, medical or whatever, out-source their data they have to ensure that the contractors meet those standards. It has also happened in the United States that out-sourced transcriptionists in India, for example, have got hold of personal data and threatened blackmail unless they are given what they want. But a sophisticated organisation can and should vet those contractors to comply with those requirements, including doing whatever due diligence and on-site review is necessary to make sure that they are dealing with people who will not steal and misuse data.
Mr Hughes: Again, in an information economy data needs to flow in order to create value, but that flow of data creates inherent risk whenever it occurs. We see it as the job of privacy professionals to manage, mitigate and reduce those risks as often as possible. A lot of our programming in countries is focused on auditing, screening and maintaining out-sourced call centres, data processing centres and things like that.

Q99 Martin Salter: In my initial question I asked you to comment on which sectors in the States in the public or private sector were more at risk of infiltration and penetration of data misuse.
Mr Gainer: I do not think the fault line can be drawn between public and private because there are numerous public organisations that have very high security, for example the defence and intelligence sectors and many others. There are now federal requirements. The Federal Information Security Management Act of 2002 (FISMA) is being enforced in the public sector. There are many state and local agencies with no security practices, so there is a huge variation across the public sector and the same across the private sector. There are private institutions that have gone above and beyond the state of the art; they are building new models for the protection of data. Some of my hospital clients are doing that. On the other hand, there are small organisations that just do not have the budget or focus to do very much at all. I view the difference in that way.
Mr Hughes: It is notable that one of the biggest security breaches we have seen in the US so far occurred with the Department of Veterans Affairs where two laptops that contained records were stolen. There was great consternation in the media and marketplace over that. I also think it is notable that the Office of Management and Budget, the oversight body for federal agencies in the United States, just this week extended notice of security breach requirements to federal agencies. Therefore, much like the private marketplace in the 30 or so states that have notice of security breach laws which require customers to be notified if data is compromised, now the federal government will be required to provide notice to citizens in the event their data is compromised.

Q100 Mr Clappison: You mentioned the way that the law operates in the United States. I want to ask about criminal penalties that are available for abuse of personal data where the type of misuse you described to us occurs. In this country the Information Commissioner has called for a couple of penalties to be available. The courts can in certain circumstances already impose short sentences of imprisonment, but the Government has said that it is looking at the strengthening of those penalties. What is your experience of this? Do you think that penalties such as imprisonment work as a deterrent? What sorts of penalties generally do you think would be appropriate?
Mr Gainer: As I mentioned in my written testimony, one of my clients had some data stolen and that particular thief was caught and sentenced to four years as a result of a federal prosecution. I do not see those types of criminal sanction as being very effective because unfortunately the criminal element never thinks that it will be caught and seems willing to take those risks. I do not think you can do away with them because you need that backstop to deter those who can be deterred. I do not believe that that is the answer.

Q101 Mr Clappison: You are saying that you need both the greater likelihood of detection and the tough penalty at the end of it?
Mr Gainer: You need detection and basically a strong defence to prevent the theft in the first place. I think a degree of prevention is called for here.
Mr Hughes: I reinforce that point. The IAPP cannot take any positions on these matters, but I am happy to share my personal thoughts. It is one thing to go after the actual fraudster who is trying to get the data to create credit card accounts and steal from people. By and large, in the United States we already have criminal law that covers all of those practices. It is another thing to create law through what some may call inspired public policy that drives better data protection and data security standards at the corporate level for those holding the data. It does not prescribe what you have to do but creates consequences, so if there is a breach it is quite painful for you and perhaps it gets you where it hurts most, that is, with your customers.

Q102 Chairman: I should like to pursue two elements of that. It has been argued to us that in the private sector the impact is the potential loss of business because customers lose confidence in a

company and that hurts, but is there any evidence of companies that have experienced serious data breaches suffering a serious loss of customers? One wonders sometimes whether this is just something that is easy to say as a way to reassure the public but it does not necessarily deliver.

Mr Hughes: I think it is a bit early. We have had these laws for only two and a half to three years, so the notices have been in the marketplace and consumers have been receiving them only for the past two years or so. ChoicePoint and TJ Maxx were the two that seemed to have the most direct connection to consumers being hurt. ChoicePoint was not a business-to-consumer business. Its business model was to sell data to other businesses and so it was difficult for consumers to have a reaction to ChoicePoint. It will be interesting to see how TJ Maxx will play out. There is a significant amount of litigation. A class action law suit has been announced and I think there will be consequences. I can offer one small personal anecdote. Earlier this year I got a gardening catalogue. As I do every year, I picked out all the vegetable seeds that I wanted to plant in my garden. About a month later I got a letter from Johnny's Selected Seeds in Maine that there had been a breach in its database and my credit card information might have been compromised. They did not know how the breach had happened, but they needed to notify me under state law. I do not think I will use Johnny's Selected Seeds again; I will use a different seed catalogue next time.

Q103 Chairman: Mr Gainer, I gather from your evidence that you suggest the focus of new regulatory powers and penalties should be on those who hold the data and allow it to be taken rather than on those criminals who steal it?

Mr Gainer: Yes, and not just an arbitrary penalty. One approach that Minnesota has adopted and other states are considering is to shift the cost of other merchants and banks that have to respond to these thefts to the business that could have done more to stop the theft instead of merchants upgrading their security, which is the only way to beat this very extensive plague of data theft. Once there is a data breach law, as there may be, we will see that just as in the States there is a huge uptake in the number of reported crimes.

Q104 Mrs Cryer: Can you talk to us briefly about the case for introducing privacy impact assessments? I understand that in the Canadian provinces of British Columbia and Ontario and also in New Zealand these have been up and running since the late 1990s. I also understand that Canada was the first national government to make such things mandatory. Take us through whether you believe these have had a measure of success and have been useful in those countries.

Mr Hughes: I can describe to you what they are and how we have seen them work in the United States. Privacy impact assessments (PIAs) in the United States have been a requirement for the past two and a half years. All federal agencies are required to have a privacy impact assessment for any programme or technology which uses personal data, and it is tied to budget so they need successfully to submit and have approved a privacy impact assessment prior to their budget being released for whatever programme or technology they are looking at pursuing. I think that if you were to talk to the people engaged in these privacy impact assessments, as I have in the past few days, they would be very supportive of and enthusiastic about such measures as a transparent tool not only for government to understand exactly what it is doing with governmental data but for privacy professionals who use this tool to assist in the development, deployment and design of these products and services and allow citizens a way to look into the operations of their government to see how things are working. I have heard from members in the United States who engage in privacy impact assessments that the process is not a point-in-time snapshot; it is not a picture of something as it passes your office door and that is it; it is an iterative process where you work on the early design stage and later you come in to work on the deployment stage. You are part of the programme throughout its lifecycle so as to ensure that not only the original design is satisfied but new issues and challenges can be addressed throughout the programme. That creates significant resource demands largely in the form of people who are expert in issues of data protection and privacy. We have found great growth in privacy professionals in the public sector in the United States who are engaged in privacy impact assessments. Even so, the Office of Management and Budget just last week reviewed the Department of Homeland Security and its efforts at engaging in privacy impact assessments. It was laudable that the department had doubled the number of privacy impact assessments that it had done in 2006 over 2004 but the numbers had gone from 11 in 2004 to 25 in 2006. In the three years it has been up and running it has done only 70 and there is a backlog of something over 100 in 2007. It is therefore a significant resource challenge for it.

Mr Gainer: One other aspect of those assessments is their impact on civil liberties groups who try to monitor what surveillance programmes are being deployed by government and how they may impact our privacy rights. When those impact assessments are done they have been used by organisations such as the Centre for Democracy and Technology (CDT) and the American Civil Liberties Union (ACLU) in the United States to find out what is on schedule for those new types of surveillance systems. When they are done they have an important benefit to the civil liberties community at least to have some window on that kind of planning.

Q105 Mrs Cryer: Do you have any information about countries that have gone down the voluntary rather than the mandatory route for PIAs? Do you know of them and, if so, how successful have they been?

Mr Gainer: I do not know.

Q106 Gwyn Prosser: Mr Hughes, with all the focus and attention on privacy-enhancing technologies, do you think there is a danger of creating a stark privacy divide between the rich and powerful who can afford privacy protection and the rest of us who have to endure surveillance and perhaps intrusion?
Mr Hughes: Certainly, I think that it is a reasonable concern and issue to look at. I would point to the fact that in a similar way to privacy impact assessments the private marketplace has largely begun privacy-sensitive development and deployment technology so that privacy-enhancing technologies are frequently baked in as opposed to bolted on; they are part of a programme or technology as it comes out of the box as opposed to something that you have to purchase after the fact. A good example of that is the Internet Explorer browser. 90%-plus of the world uses the Internet Explorer browser. I am sure there are many arguments about whether or not that is appropriate, but the fact is that it has very strong privacy protections within it. Many of the technologies within the browser that are of concern to consumers and privacy advocates—things like cookies—are incredible tools to manage those functions that are built right into the Internet Explorer browser. Privacy professionals are now very active not only in demanding compliance with law from their organisations but also working their way into design and development teams so that those designs are built with privacy at the very start baked into the DNA of the product or service.

Q107 Gwyn Prosser: Do you think that legislation and regulation can keep track of the acceleration in new technologies on both sides of the argument with respect to both the use of information for criminal purposes and the protection of privacy where you come from?
Mr Hughes: Again, that is a very simple question that could lead to a very long and protracted discussion. As a personal opinion, I think we have seen examples where laws that try to target a specific technology find that the technology shifts, or the fear associated with that technology or its misuse goes away because the law covers it up but fraudsters just move to another technology that is right next to it which has not been covered in the original law. One thing I am certain of is that technology changes very quickly. We see that every day and every month and it is very challenging to try to approach privacy protection in a *post facto* way, always chasing the latest technological development. As privacy professionals we struggle with getting our heads around how data is used in every new technology that emerges. I think it is even more challenging to try to think of legislating or providing regulatory controls round all those things. For that reason we have seen many jurisdictions focus not so much on the technology itself but the use or misuse of the data and defining what data should be within scope and then putting parameters on uses or misuses of that data.

Q108 Mr Benyon: Recent reports in the media in the UK have highlighted concerns about the capacity of companies such as Google to use data to create profiles of their customers. Reacting to that, Google has said that, for example, it would anonymise information it had gathered from searches after 18 to 24 months. How much confidence do you as privacy professionals feel we can have in decisions to anonymise or reduce the amount of data that organisations such as Google hold on us?
Mr Gainer: You can have some because, first, it is in their interests to avoid regulation about discarding data. The reason that Google's search engine works so well is that it uses those saved searches at least in part to refine the algorithms for that search engine, so it needs to retain some data for that purpose and also for other marketing work. If anonymisation permits them to retain that without the fear many people have that those types of personally identifiable searches will be misused then they have an incentive to do the anonymisation.
Anonymisation is a very good tool in many contexts to protect the privacy interests of all of us who are subject to this exploding technology. I do not think it is enough to say that it is moving so quickly we cannot regulate it. As policymakers, it seems that it is a choice of how to regulate because it affects privacy rights so significantly. I think that Google will anonymise its data. I think that it could be imposed on companies so they anonymise data to ensure that those kinds of personally identifiable and very sensitive searches are not misused.
Mr Hughes: I have great confidence that Google will do what it says it will do. I should note that Google's privacy officer, Peter Fleischer, is on our board of directors. One of the reasons I have great confidence that Google will do what it says it will do is that it has privacy professionals on its staff and the consequences of them failing to live up to the promises they have made to the marketplace are dire indeed. In the United States we most definitely have a compliance culture and a statement unilaterally made through a privacy policy can be used against you under the FTC Act. We have seen that in many circumstances.

Q109 Mr Benyon: So, if the company says something in the form of self-regulation and does not achieve that it can be found to have broken the law?
Mr Hughes: Most assuredly, yes.
Mr Gainer: And not only by the FTC but often in private litigation. We face a lawsuit where one of our clients made a representation in a privacy statement. The plaintiffs claim that it was not carried through and they seek damages for that failure to comply.

Q110 Mr Benyon: It would be interesting to know whether there is similar rigour in our compliance, but for the sake of time I will move on. You have described how privacy professionals work. I think that you have described it as being part of the DNA of the project from start to finish so advice can be given as to whether a company is likely to be over-intrusive into people's private lives or to be at risk of breaking the law. But in your experience how many

companies have a designated board director responsible for privacy? What influence does a privacy officer have, for example over a CEO of one of your client companies?

Mr Hughes: It varies. I am not aware of structures where a member of the board is given specific responsibility for privacy. I am aware of a limited number of situations where the chief privacy officer has the ability or is required to report to the board directly, but also report from a management perspective through the CEO. Chief privacy officers, like chief compliance officers, general counsel, chief risk officers and many others in organisations, work within a management structure. Sometimes they have to work by influence, strategy and cajoling and sometimes they have to have a backbone and stand up for what is right within an organisation. I think that in the United States we have a compliance culture, which is particularly driven by Sarbanes-Oxley, where organisations are very concerned about compliance issues that may not be resolved within the organisation because under that Act they would have to report those in their public reporting. That may be a mechanism that has reduced the need for privacy officers and professionals to have direct board access, because if there is a problem then theoretically that goes to the board anyway.

Mr Gainer: My one client who has done the most in imposing new security measures did so because the head of the audit committee on the board required it. Therefore, it became a top-down mandate that was monitored by the audit committee. That kind of interest and leadership by the board of the organisation, which was a state hospital with hundreds of facilities, has done a remarkable job of improving its security.

Q111 Chairman: Many British companies would regard themselves as dangerously exposed legally if they did not have a board director responsible for health and safety compliance. Given the importance of the issues that we have been talking about this morning, do you see a point in future when companies would routinely have a board member with direct responsibility for these issues?

Mr Gainer: That is a natural outgrowth of the audit committees which are saddled with important Sarbanes-Oxley reporting requirements. If the organisation is not complying with privacy laws then that becomes a matter that may need to be reported by private companies in their statements to the SEC. I think that is a natural progression.

Chairman: Gentlemen, thank you very much. You have been enormously helpful and also very clear this morning.

Witnesses: **Mr Mike Bradford**, Director of Regulatory and Consumer Affairs, Experian, **Mr Stephen Sklaroff**, Director-General Designate, Finance & Leasing Association, **Mr Martin Briggs**, Corporate Affairs Director, Loyalty Management Group, and **Mr Nick Eland**, Legal Services Manager, Tesco, gave evidence.

Q112 Chairman: Gentlemen, thank you very much for coming. This is part of an inquiry to explore the Information Commissioner's claim that we are moving towards a surveillance society and, if true, how we should respond to it. Perhaps each of you would introduce himself for the record and then we will get the questioning under way.

Mr Sklaroff: I am Stephen Sklaroff, Director-General Designate of the Financing & Leasing Association with which I have been for a total of three weeks. I am very pleased to have the opportunity to come along to this hearing.

Mr Briggs: I am Martin Briggs, Corporate Affairs Director for Loyalty Management Group, the holding company of the group which owns and operates the Nectar loyalty programme.

Mr Bradford: I am Mike Bradford, Director of Regulatory and Consumer Affairs at Experian, and President-elect of the Association of Consumer Credit Information Suppliers, a European body of credit reference agencies.

Mr Eland: My name is Nick Eland, the Legal Service Manager at Tesco. I have also spent a fair amount of time doing data protection management within the business.

Q113 Chairman: I am sure that a number of our questions would be of interest to each of you, but we will try to direct questions to the particular individual concerned; otherwise, we will duplicate quite a lot of areas and not get through all the issues that we would like to cover. I begin with a general question to Mr Bradford. When you produce credit files which contain information from lots of different sources—the electoral roll, county court judgments and so on—what is the process by which the data from those different sources is drawn together in compiling those credit reports?

Mr Bradford: If I may start by explaining what a credit reference agency does and how the information is compiled that will probably put it into context. Experian as a credit reference agency sits between the lender and the consumer. The consumer will be looking for speedy access to goods and services at a competitive rate and equally a lender needs to make a responsible lending decision. The information that Experian or a credit reference agency holds is effectively very often the information that has been provided by the consumer himself by direct consent to Experian and other publicly available data sources such as the electoral register and county court judgments. Therefore, within the credit bureau the information is held either because it is publicly available or because through a lender or third-party source the consumer has given his agreement for that data to sit in a credit reference agency. A consumer may come to Experian and ask to see his or her credit report. Interestingly, there is a lot of awareness of this because part and parcel of our consumer affairs function is to ensure that consumers are aware of their rights and how they can look at their credit information. Therefore, the credit reports that we

produce—we produce more than a million consumer credit reports every year for consumers in the UK—will consist of details of credit agreements that they have with lenders and any organisation that has searched their credit file, so they have an audit footprint. Again, for transparency if an organisation has looked at a consumer's file the consumer will see that recorded on the file. They will see any relevant information relating to county court judgments, the electoral register and so on. If there is a financial relationship with their partner—perhaps they have a joint mortgage or credit account—they will see the name of the person with whom they have that relationship but not that person's data because that data belongs to that other person from a privacy point of view. That is basically what a credit file looks like. We have statutory turn-around times to produce that information. As a credit reference agency, we have statutory obligations to deal with consumers' queries about their credit reports. I believe that last year we had about 900,000 or so consumer interactions on that basis. We employ 200 people who are dedicated to servicing the consumer part of credit referencing.

Q114 Chairman: Mr Sklaroff, for whose benefit is all of this done—for me as a consumer or you as a lender?
Mr Sklaroff: I think that in this case it is for both. This is one of those instances where the interests of the consumer and the lender are the same in the sense that the lender wants to be in a position to lend responsibly to a consumer. It is not in the lender's interests for consumers to become over-indebted and even further stretched. It is in the consumer's interest that the lender should have access to relevant information which bears on that point. By the same token, the information allows lenders to intervene with consumers and talk to them if it appears that the consumers are, to employ an expression used in the industry, at the tipping point, that is, in a situation where they have what appears to be a manageable amount of debt but may be trying to contract for too much which will take them into a situation of over-indebtedness. There are things that the lender can then do. Therefore, the data that my colleague has just talked about is crucial to that process. The other two reasons why the lenders are interested in the data are the prevention of fraud and money-laundering. The same data serves those three purposes. Therefore, one is concerned on the one hand with responsible lending on the other with the prevention of crime.

Q115 Chairman: You make it sound quite benign when it is put like that, but if government came along and said, "We are going to look at your bank account and see if you are getting into too much debt", there would be absolute outrage and reference to the nanny state. Is it acceptable for a private sector company to have such a paternalistic view?
Mr Sklaroff: I believe that in this case "benign" is the right word, because this technology and the existence of CRAs has come about because the credit market is now very different from what it was perhaps 30 years ago. Then one's only way of getting credit in the legitimate regulated market, to put it that way, was to go to the local bank manager who would bring to bear to his decision whether or not to lend any personal knowledge he might have about the applicant or his family. The bank might have known you for some time and so could judge whether or not you would be a good credit risk. There are huge advantages to the consumer in the situation we now have where it is not reliant on that kind of immediate personal knowledge; it is a little more anonymous. But in order to make that system work one has to have reliable data on which the lender can draw in order to make a decision. I think that it is benign in the sense it benefits the consumer.

Q116 Mr Winnick: Is not the criticism somewhat of the opposite kind, namely, that people whose financial situation is pretty dire get hold of credit cards? For example, we read in the press that people go into bankruptcy having messed around with one or another card and built up huge debts. Therefore, the accusation could simply be that not enough care is given before issuing a credit card. Do you accept that criticism as justified?
Mr Sklaroff: I think the point is an extremely important one. In some ways this was exactly what I was trying to say. In order to detect when that kind of situation occurs this data, properly controlled with the right kinds of checks and balances, needs to be shared so that a prospective lending company when presented with a customer who says he would like another credit card or take out further credit for the purchase of a car or whatever it is, can be in a position to say that on the basis of the information available he believes the consumer is getting himself into trouble. There are then things that the lender can do in conjunction with the customer to try to put that right.

Q117 Mr Winnick: That is all very well. The inevitable question is: how does a situation arise in which people with a good number of debts go from one card to another accumulating five or six accounts, despite the fact that clearly their financial situation is as I described in the previous question?
Mr Sklaroff: What you describe there is a symptom of the fact that there are still things that we need to do to make the data exchange process more efficient, accurate and contain more information that is relevant to the lender.

Q118 Mr Browne: When people apply for loyalty cards and such like what information about them do you collate? For example, do you know what they buy and in what combinations and when they buy it so you can track whether or not they purchase things in the middle of the night? For example, if the customer is a lorry driver you will be able to track his or her movements around the country, or even abroad if you have stores overseas? Is that true? Do you collate all of that information on each individual?

Mr Briggs: It may help if I outline exactly the information that Nectar collects. When consumers register for Nectar for the first time we take basic contact information so we can operate the account and issue points and redeem them when consumers want to use them. We also collect some fairly basic lifestyle information including how many adults and children there are in the household, how many miles might be driven in a year and information like that. We also ask for security information so that the account can be operated securely by way of, say, a memorable word or password. That is the information we collect when people register with the programme. When people use their cards we collect the following information which is not as detailed as you have just outlined. We collect information as to where somebody has shopped, the date and time they have shopped and the total amount they have spent. We do not collect information as to exactly what that money has been spent on. To give an example, if I went to the Westminster branch of Sainsbury's this morning before coming here you would know that I had gone to that branch on 7 June at 9.30 in the morning and had spent £10 and so I should be issued 20 points but we will not know what I have bought.

Q119 Mr Browne: I would not know that you had bought incontinence pads and Horlicks; I could not draw a conclusion that you would shop for products that would be likely to be bought by older people, for example?
Mr Briggs: Correct. We do not take that information.

Q120 Mr Browne: Is the same true for Tesco?
Mr Eland: It is very similar. There are two main routes by which we collect information.

Q121 Mr Browne: Would you know that a person had bought chocolate bars?
Mr Eland: We do collect transactional data of each customer. The main routes by which we collect the information are the application form—the key thing is the name and address—and, when they use their Clubcard in store, we can see what they have bought whilst they have been in the store.

Q122 Mr Browne: I assume that that is the crucial information because you can use that information to build up a profile about different categories of consumers who are likely to buy goods in different combinations and then market things accordingly?
Mr Eland: Indeed. It is crucial to the programme. It is a loyalty scheme which obviously customers choose to join. It offers them benefits, but to offer them we need a certain amount of information to ensure that the way we communicate with them and market to them fits what they want to hear and see.

Q123 Mr Browne: Therefore, the example that I gave a moment ago, which was not particularly sensitive, would apply in your case. You might want to come up with another example, but it still holds true that you would build up a profile of the type of person. You could probably make some fairly safe assumptions about the individual based on his or her buying patterns?
Mr Eland: Yes. We collect all their data and create profiles about those customers better to understand their behaviour, again to ensure that when we do contact them we do so for the right purposes and in relation to products that would be of interest to them.

Q124 Mr Browne: For how long do you hold this data? Let us say somebody has bought something they consider embarrassing or he would rather people did not know about it, albeit it is a legal product in one of your stores. Would it be possible that five or 10 years later that would still be known about?
Mr Eland: We keep the data for a maximum of two years so we have full transactional data on our customers.[1]

Q125 Mr Browne: Are there any circumstances in which you might considering sharing it? One would have to be a fairly slow-witted fugitive who went round the country using a loyalty card, but nonetheless I am sure that some would have those features. If the police said that they were trying to track someone and it would be helpful to have a sense of where they might have been in the country over the past month, or perhaps to test alibis—for example, somebody who has given his assurance that he has not been anywhere near the West Midlands in the past six months—would you be willing to impart information showing that that individual had used one of your cards in a Coventry store?
Mr Eland: We do. There is a clear legislative requirement in terms of how that information would be provided under the Data Protection Act and RIPA. It is probably worth putting it in context. We have 30 million active customers and I believe that in the past year we have had fewer than 200 total requests. The majority of those are from customers themselves under the subject access process.

Q126 Mr Browne: Would you give details of individual items? Let us say it is relevant to a court case. Assume somebody has denied being on a certain diet or has been of a certain weight. I am trying to think of a good example. Let us assume the person has bought some pornography, or whatever else it may be. You may disclose not just the location. If the individual items the consumer has bought are relevant to the case you will be willing to share that with the police, subject to the criteria that you explained?
Mr Eland: I think the process is that a request is made by the police and we will respond to that. There is no obligation to provide it, but my understanding is that in the long term they can acquire it ultimately through a court order. The

[1] *Note by witness:* We only use transactional data of Clubcard customers for a maximum of two years. Beyond this point, the data is anonymised and is not attributable to an individual Clubcard customer.

approach we take is to ensure that the request is justifiable and, more importantly, that it does not require more data than is necessary for the purposes they require it. We will then make a decision as to whether we think it is appropriate to pass on that data.

Q127 Mr Browne: It is an interesting distinction. The previous witnesses said they thought that the difference between the United States and most of Europe including Britain was that here we were reasonably relaxed relative to the Americans about the state having information about us but we were relatively guarded compared with Americans about private companies having access to information about us. Perhaps their suspicion of big government looking at information was the other way round. You are saying that people should not assume there is a wall dividing the two and you are willing to co-operate with the state, maybe for very good and laudable objectives, but when people use your cards they should not think that that is entirely about commerce, vouchers and all kinds of bits and pieces like that; it will potentially go on the other side of the divide and be used by the police or other authorities if need be?
Mr Briggs: To clarify that, I think that the statutory requirements are slightly more limited than you suggest. The Data Protection Act includes a specific exemption to enable organisations to disclose information for very limited purposes, including the detection and prevention of crime and catching a suspect. There are various restrictions imposed on that particular process on which the Information Commissioner's Office has issued very helpful guidelines. First, it requires that request to be validated so as to ensure it is coming from the purported source. The request must be seen as a specific one, not just a fishing expedition. Therefore, in terms of the example you have just given where people may have been touring the country that request would probably not be met. Once those requirements have been met the holder of that data must decide whether or not it would be prejudicial for the purposes of the prevention or detection of crime to disclose that data. This applies in very limited circumstances, which would basically be the investigation of criminal activities. It is not just a general permission to disclose everything that we have to any government agency that may wish to receive it.

Q128 Mr Browne: On a similar note, because Nectar cards have different outlets and different companies band together as part of the whole scheme, how much data is interchangeable between them? For example, if I never buy petrol from BP because I have some reason not to do so but I often shop at Sainsbury's would BP still have the information about my shopping patterns in case they wish to entice me to buy petrol from them, knowing that the nearest petrol station to Sainsbury's that I go to regularly does happen to be a BP station and I am missing out by not using that garage?
Mr Briggs: The purpose for which we collect consumer data is basically to be able to track people's shopping behaviour and to be able to market offers that they will find acceptable.

Q129 Mr Browne: So, BP would have information about my buying patterns, despite the fact I had never bought anything from BP ever, if I bought something from Sainsbury's or one of the others involved in this scheme?
Mr Briggs: No; that is not the way our programme works. Clearly, at a commercial level no major organisation will allow its valuable customer data to be given over to a whole number of other companies just because they happen to participate in a programme like Nectar. The way we operate is that the Nectar database is owned and operated by Nectar. The information that we collect on, say, a BP customer is clearly available to BP and maybe we will carry out analysis on that data to enable BP to send offers that it may wish to give customers.

Q130 Mr Browne: Perhaps I am being slow-witted. To go back to your earlier example, Westminster Sainsbury's will know that you went there at 9.32 in the morning, or whatever. Only Sainsbury's—no other company—would know that you went there at that time and used your Nectar card?
Mr Briggs: That is correct.

Q131 Mr Browne: As far as concerns Tesco although it is increasingly diversifying into areas like insurance people tend to think of it as a traditional grocery retailer. If they know that I am buying broccoli at the same time as I buy a Mars bar it does not matter greatly, but people may have slightly different views if it is about financial services. Is all of that kept and collated in the same way?
Mr Eland: They are very much stand-alone systems. The bottom line is that with the broader retail services that you refer to—take Tesco personal finance—the majority of data in relation to Clubcard is the flow of information from TPF to Tesco for the purpose of running the Clubcard scheme. One can obtain points through using a Tesco credit card, for example, and those points would need to flow to Clubcard so we can reward our customers.

Q132 Mr Browne: But they are not cross-referenced. Let us take an insurance form that I have to fill out with my health details, for example whether or not I smoke. Would you be able to cross-reference that against my buying patterns which show that I buy endless packets of cigarettes from your stores?
Mr Eland: We would not, and "would not" is the key point.

Q133 Mr Browne: You could but you would choose not to?
Mr Eland: The scheme relies on customers trusting us and valuing the scheme. In our view, those kinds of actions would massively reduce that trust and, therefore, would not make the scheme effective. It is there to reward our customers primarily and,

therefore, the concept of that sort of exercise would just damage the trust of the customers that shop in our stores.

Q134 Chairman: Why not just do green shield stamps, which was what you were accused of doing when you first introduced the Clubcard? Why not have a loyalty system that does not require millions of customers to give their names and addresses?
Mr Eland: The name and address is fundamental to us to be able to run the scheme. We need to be able to send out statements quarterly with the information attached. The application form itself can minimise that to the name and address so that all we have is the name and address and the information we collect in relation to the actual transactions. Wherever possible we try to minimise the data that the customer has to give us to be part of the scheme.
Mr Briggs: We find that a lot of customers wish us to have their name and address. Strictly speaking, in Nectar you do not have to provide your name and address. Obviously, we wish people to do so because we want them to benefit from the programme, and consumers know that to benefit from the programme they need to provide contact details. To give an example, every year our customer service team receives about two million letters, phone calls and emails. Last month about 30% of those were people basically telling us about changes to their details so they could be contacted properly. It is something of which consumers see the benefit and in which they wish to participate.

Q135 Mr Winnick: There seems to be concern about data sharing between the private and public sectors for the apparent purpose of tackling crime. To what extent do you say that consumers and borrowers are aware that this data-sharing is taking place?
Mr Sklaroff: There is a very interesting issue about the general level of education of the public about individual's rights and responsibilities under both the Data Protection Act and more generally with regard to the whole set of issues that we are discussing today. I think that more can be done sensibly to ensure that people are aware not just of what the data they have provided is being used for but also that they understand what they can do to check that data, get access to it and make sure that if corrections need to be made they are made. In response to your general point, I think there is more to be done. For example, I know that the Information Commissioner is doing work on this at the moment. Leaflets for consumers are already available. My own association produces such consumer information, but I think more can be done. On the same point, at the moment there is a great and laudable push on the part of the Treasury, the Financial Services Authority and others to raise the general level of financial education in the population at large. There may be lessons to be learned from that process with regard to owning and being aware of one's own data and understanding what it is being used for.

Q136 Mr Winnick: The truth is that the organisations which you represent have as much information about all of us in this room as state agencies such as the Department of Social Security and the rest. Is that not the case?
Mr Sklaroff: The truth is that the data that is gathered is different for different purposes. As you say, there is a very legitimate debate to be had about the overlap and interchange between public and private databases, but, to pick up the discussion we just had, the rules which govern the interchange of information about credit reference agencies whom Mr Bradford represents are absolutely clear that that data may be requested for two purposes only: to ensure that people do not become over-indebted and to prevent fraud. On the point about cross-marketing, it is expressly forbidden.
Mr Bradford: In the hope of putting your mind at rest, the private sector does not hold the same amount of information that perhaps the public sector holds. If I look at what a credit reference agency holds in the UK, it is effectively your credit information that you will have known is going into a credit reference agency and some publicly available information like the electoral register and county court judgments. We certainly do not have access to DSS-type social security information and so on. To go back to the previous comment about public/private sector data exchange, one thing perhaps we need to be very aware of from the commercial perspective is that we rely very much on trust and transparency. I am sure that there could be legitimate purposes for exchanging information between the public and private sectors, subject to the very strong caveat that the consumer is aware of what is going on, why it is needed and that it is only for legitimate purposes. I know that Richard Thomas is very concerned in some public sector data-sharing about purpose creep. You provide information for one purpose and suddenly it finds itself doing something else. From a private perspective we literally cannot do that. When it comes to public/private data-sharing that same caveat must apply very much. Consumers need to be aware of what happens.

Q137 Mr Winnick: The Information Commissioner has expressed doubts about the benefit of increased information sharing in view of the dangers to individuals' privacy. Are you having meetings with him to discuss this?
Mr Bradford: A critical part of my team's role within Experian is to meet with Richard Thomas and his commissioners usually about three or four times a year to discuss what we do to ensure that they are comfortable with what we are doing with personal information. As to private sector/public sector data exchange, at this stage it is not something about which we have had a specific discussion.

Q138 Mr Winnick: Mr Eland, in the paper that you have circulated you refer to the analysis of Tesco Clubcard being managed by Dunnhumby. You explain why and so on. In the course of that document—this is related to some extent to the

questions put by Mr Browne—you write: "At no stage do we ask Dunnhumby to analyse information on individuals. This information is accessed only at the request of the Home Office or the individual customer." Leaving aside the individual customer, what is the relationship between the information that you collect and the Home Office?
Mr Eland: The information that we collect is for the purposes of running our scheme and to ensure that we are marketing customers properly and getting a better understanding of customer behaviour within our stores so we can improve the service we provide to them. In terms of that statement, the point we try to make is that Dunnhumby does a lot of analysis on anonymised data; it is not looking at individuals but trying to look at broad ranges of customers as a whole better to understand their behaviour and enable us to achieve the goals of the scheme. The comment about the Home Office arises simply because in relation to subject access requests and the requests by the police that we talked about earlier Dunnhumby might need to provide some information back to Tesco for the purpose of meeting those.

Q139 Chairman: If I buy a lot of wine from Tesco will you try to sell me more wine?
Mr Eland: We would probably send a wine coupon, if it was relevant.

Q140 Chairman: In view of the Government's alcohol strategy this week, is it a good thing that you analyse somebody's consumer patterns? What if I eat a lot of Turkey Twizzlers? Would you like to sell me more? This is a serious issue. Mr Sklaroff is very keen to tell us that this data is used in order to benefit the customer and prevent him getting into debt. I do not quite see why Tesco should be trying to raise the consumption of high-fat, high-salt or alcohol products because those are the things that somebody is already buying. Beyond selling as much as you can of whatever harmful product it is the consumer is buying, where is the level of responsibility to stop?
Mr Eland: I think the answer is that we constantly contact and speak to our customers to understand whether what we are sending is appropriate to them. If we fail to do that our customers would let us know by not using the scheme.

Q141 Chairman: I may be an alcoholic. It may be that to send me wine vouchers is not a particularly benign thing to do.
Mr Eland: We recognise that there are certain areas of concern. We would never promote tobacco or baby formula or those kinds of areas. I appreciate the point you make, but we are running a loyalty scheme and ultimately we have to rely on our customers to make the decision in relation to the information and the offers we provide to them.

Q142 Mr Winnick: As far as concerns the information collected by Dunnhumby, is the position that the Home Office may at some stage, perhaps for very good purposes, say to Dunnhumby that it has collected information from Tesco customers for the purposes of the Clubcard and the department requires such and such information from that company? If not, I do not understand—perhaps it is my misreading—"This information is accessed only at the request of the Home Office or the individual customer." There must be some sort of relationship, otherwise you would not have put that in the document with which you have supplied us, between Dunnhumby and the Home Office.
Mr Eland: I reiterate the point. I believe that the point we were getting at was that Dunnhumby analyses data at a non-personal level. It holds information and ultimately if a request is made by the police or customers we can provide that to them in accordance with a subject access request process. I do not believe that that suggests in any way that there is some kind of wholesale sharing of information with the Home Office.

Q143 Mr Winnick: If not wholesale, some information?
Mr Eland: No, there is not, other than the subject access process and the occasional police request.

Q144 Gwyn Prosser: Mr Briggs, I am tempted to ask you what you did buy at Sainsbury's this morning. I take you back to what the Information Commissioner shared with us when we talked about our concerns about the security of information kept on us by the private sector. He said that there were enormous commercial self-interest pressures in the private sector to hold that information to itself because it is so valuable. That seems to be a commonsense response, but what evidence is there that that commercial pressure is sufficient to keep that evidence safe and secure?
Mr Briggs: The trust of consumers is absolutely fundamental to programmes such as ours. Our programme is a voluntary one. People register for the programme because they wish to benefit from it. They have the choice of deciding how much information they provide to us; they have the choice of deciding whether or not that information is to be used for marketing purposes and how it is to be used for marketing purposes. They can choose if and when they use their card to collect points and use them. They can opt out of marketing at any time. All of these things are hard-wired into the system. The trust in our complying with all of those requests is absolutely fundamental. If people did not believe that we were fulfilling that correctly they would vote with their feet. Another question that came up this morning was whether or not data had responsibility at board level. I can say that in our company it absolutely does. A director on the main board has responsibility for data issues. Data is our business; it is what we do. It is absolutely fundamental to getting it right that the trust of the collector is enhanced. In terms of security of data, data is held securely in a number of ways: there are IT and system measures; there are policies and procedures which are requirements within the business; and there is also the cultural issue of how we train people in the business. I can go into all those in more detail if you

wish, but all of those matters are absolutely hard-wired into the way we do business. We are a commercial organisation and if we do not get it right we do not make money.

Q145 Gwyn Prosser: Mr Eland, what impact study has Tesco carried out into the effect on the company of losing this detailed personal information?
Mr Eland: What do you mean by "impact study"?

Q146 Gwyn Prosser: Have you looked at the impact it would have on your business if the information that you hold on consumers, including in your case details of purchases, became available to others?
Mr Eland: Our focus is to ensure that that data does not become broadly available.[2] I reflect the comment—I know we say this time and again—that trust is key. Part of that is our customer feeling secure in the knowledge that his data is used by Tesco for the purpose of running its loyalty scheme. Any failure to do that obviously would damage the scheme. On top of that, we have in place the security measures to which my colleagues have referred to ensure that that data is physically secure. I am not aware of any intention to release that data in any way in a broad sense, so if that ever did arise due to a requirement by way of legislation perhaps we would have to revisit that point and consider it.

Q147 Gwyn Prosser: In terms of safeguarding personal information, do any of the witnesses have any strong ideas in which areas the Government could learn from the private sector?
Mr Bradford: Very much so. The private sector has run secure, trusted data-sharing protocols now for 30 years in the UK to the consumer's advantage. As to the security issue, I am sure that any data controller including a government department is aware of its obligations and, hopefully, of what good data security protocols are in terms of encryption, ISO standards, BS standards and so on, which are certainly matters to which Experian subscribe. I think that perhaps the more private and public sectors can meet to discuss and review these areas the more it is to the mutual advantage of both sectors and, at the end of the day, the consumer.

Q148 Martin Salter: My question is probably best directed to Mr Briggs and Mr Eland. I should like to pick up the Chairman's question about whether you should just sell green shield stamps. It seems to me that you could interpret your need for identity effectively as buying names and addresses for your customers, and the by-product is that the incentive for people to hand over that information is that they can shop at a cheaper rate. How far do retailers go down the road of saying to people that there are limits to the information that they have to hand over, though obviously for commercial reasons you want them to hand over as much information as possible so you can develop market profiles? I know that the Information Commissioner has expressed some concerns about this. Do you have any plans to make it much clearer—in other words, in type slightly bigger than eight point—that when people sign up for a loyalty card there are a number of boxes they can tick to prevent personal information being shared with you as undoubtedly responsible organisations?
Mr Eland: For me, an example would be the time we relaunched our application form. At that time we talked to customers about what concerned them in terms of understanding what Tesco did with the information. As a result of that, our application form has primarily optional fields. We collect only the key information that is necessary to run the scheme. We also talked to them about the data protection statement in order to get a better understanding of that. The example that comes to mind is that at one particular customer question time we made reference to aggregated data and a customer asked whether that had something to do with concrete. We try to make sure that our wording and the way we set out our statements is much clearer to customers so they understand what we are doing with the data.
Mr Briggs: That is absolutely the case with Nectar as well. When customers sign up for the programme there is a clear statement as to the data that is collected, to whom it will be disclosed and how it will be used. For example, we do not sell data outside the Nectar programme; it does not go to companies that buy and sell lists. We make that absolutely clear. It is not just a legal requirement; it is a commercial requirement in terms of building trust with the customer. Slightly implicit in your question is that somehow consumers are required to give this data. This is a voluntary programme. If people wish to benefit and receive offers they have to tell us where they are so they can receive them.

Q149 Martin Salter: Is it correct that you can have money off your grocery bill as a result of participating in a store card scheme but only if you hand over your name and address?
Mr Briggs: Yes, but there are so many things from Nectar other than money off your supermarket bill.

Q150 Martin Salter: For most of my constituents, to save some money by signing up for a store card is a fairly strong incentive.
Mr Briggs: Absolutely.

Q151 Martin Salter: If you do not hand over name, rank and number you do not save money, basically.
Mr Briggs: But you can get far greater value out of Nectar by using your points for things other than supermarket shopping, for example having days out at Thorpe Park, free cinema tickets and that sort of thing. You get much more value out of your points than just taking them along and getting money off your shopping.

[2] *Note by witness:* We work extremely hard to ensure that such data does not become available to any external organisations. We recognise the importance of keeping our customer data secure and confidential and work extremely hard to achieve this.

Q152 Martin Salter: I am sure that it is a life-enhancing experience, but what proportion of your customers choose to redeem their points financially, as opposed to those who decide to have a day out at Thorpe Park or take advantage of the other goodies that you have on offer?
Mr Briggs: In general terms, seven out of every 10 of our collectors have used their points. We have provided back over £800 million worth of value to collectors since we launched the programme four and a half years ago.

Q153 Martin Salter: That is not my question. My question is how is that £800 million split? How much is accounted for by people seeking money off their grocery bills and how much by them taking advantage of the other goodies that you have on offer?
Mr Briggs: I do not have that—
Chairman: We are moving slightly away from surveillance and into a commercial area.
Martin Salter: I will put one further question and then stop. Some of the products that one buys at stores can be intensely personal, for example medical or contraceptive devices or whatever. All that information becomes available. If somebody wants to opt out of providing that information to you how can he do so?

Q154 Mr Benyon: Pay cash.
Mr Eland: Or not join the scheme.

Q155 Chairman: To pursue one further point, somebody wants these benefits, but, as I understand it, certainly Tesco and possibly Sainsbury's or Nectar may use the information to identify where there is a large group of Tesco customers but no local Tesco store. Is that right? As a customer I may not want my shopping patterns to be used to have my own district shopping centre put out of business by a new superstore. First, if somebody signs up for a card does he know that that information may be used for strategic planning purposes by the company? Second, can that individual opt out of having that information used in that way? Is there anything explicit that says it can be used in that way?
Mr Briggs: That is not something that applies to Nectar. Sainsbury's may have its own data and use that for its own purposes. All Nectar is concerned about is having information about shopping behaviour so it can market offers to customers.

Q156 Chairman: Sainsbury's does not draw on the Nectar card data to know the locations of its customers and how much they spend?
Mr Briggs: They will know from our data what a consumer has spent at a particular time at a particular place.

Q157 Chairman: Therefore, it could use it for strategic planning purposes?
Mr Briggs: If it wished to do so, yes.

Q158 Chairman: And Tesco?
Mr Eland: Because of the nature of the data we can certainly use that to understand local demographics. One point I raise is that where one uses customer information customers have already shown a preference for Tesco.

Q159 Chairman: I may well want occasionally to stop at a supermarket and also want a local district shopping centre. My point is that it is never explained to me that this may be used to put my local district shopping centre out of business and how I can opt out of my data being used in that way if I want to do so.
Mr Briggs: That is not something for which the data would be used under our Nectar data protection policy. If Sainsbury's uses data information it received by virtue of its point of sale it may do that; I do not know. You will have to ask Sainsbury's.

Q160 Chairman: Sainsbury's could not retrieve a geographical analysis of its Nectar card users' home addresses in order to use that for its strategic planning purposes?
Mr Briggs: Our data protection policy says that the information will be shared so as to market goods and services which may be of interest to the consumer.

Q161 Chairman: Tesco Clubcard information could be used in that way?
Mr Eland: The answer is that Clubcard information is used primarily for the running of the scheme and for the benefit of customers. That applies across the board. I cannot give you further detail about how our insight units may use it in the ways you suggest.
Chairman: If after this session there is any further information that you want to provide to the Committee on how this data is used and whether the customer has any control over it that will be very useful.

Q162 Mrs Dean: Mr Sklaroff, can you say how accurate the data used by credit reference agencies is, and has it become more accurate over the years?
Mr Sklaroff: I believe that it has become more accurate over the years because more effort has gone into ensuring that it is captured and transferred in ways that are less prone to error. This is something which the industry is keen to improve constantly because there is a clear commercial interest for the industry as well as the concerns that we are discussing today to ensure this information is accurate. If it is not, the very purpose of gathering it in the first place from a commercial point of view is undermined. If one is not getting a sufficiently clear picture of one's potential clients' credit situation, for example, one may very well end up making the wrong kinds of decisions which commercially is not an attractive situation in which to be. It is a continual process of improving the quality of the data and is something about which the industry is very concerned.

Mr Bradford: Looking at it from a credit reference agency point of view, the data we hold is effectively gathered from a number of sources, one of which is lenders. From the point of view of credit reference, we have seen significant improvements over recent years in the quality of data that comes in from the industry and third parties, for example the voters' roll and so on. There are two drivers for that: one is the commerciality of it, because at the end of the day the data needs to be as accurate as possible to be of optimal value; the other is the realisation under the Data Protection Act in particular that there is a stringent requirement for data to be accurate and up to date. Over recent years with the Information Commissioner's Office we have done a lot of things to improve both the accuracy and amount of information. The Information Commissioner's Office has a requirement that when a record goes into the credit bureau it is not just "M Bradford" with a postcode; it must be fully populated with the title, full forename, surname, date of birth and so on so that accuracy is guaranteed as it comes into the bureau.

Q163 Mrs Dean: Is one of the problems the source of income? If somebody pays off a credit card debt you do not know whether that money has been borrowed for that purpose. We all know that if someone does pay off a credit card debt he or she will be offered even greater credit. Is one of the problems that you are not able to assess where someone's income comes from?

Mr Sklaroff: You have put your finger on a very important issue. This goes to the point on which we touched earlier about the quality of the data. The better the coverage of the data in terms of the financial status of the individual the more useful it is for these purposes and the better able is the lender to say that from the information available it appears that the consumer should not really be contracting the credit agreement, or whatever it is. I very much agree that what we in the industry are trying to do in conjunction with credit reference agencies and in discussion with the Information Commissioner and others is ensure that we have access to the right and relevant kinds of data to help us do that. There are categories of data which at the moment are not available to the industry. We have welcomed recent consultation issued by the DTI on the subject of historical data which predates the introduction of the current system of fair processing notices and letting the customer know that his data will be used for this purpose. There are about 40 million transactions out there that we know exist but which are not part of the sharing process. It seems to us that, in precisely the way you suggest, this is relevant information if used properly for the restricted purposes we are talking about. Therefore, we are keen to get access to that.

Q164 Mrs Dean: Mr Bradford, you mentioned earlier that there was an increase in awareness of credit reference agencies. Would you welcome or resist moves to require credit reference agencies actively to inform people what data was held about them?

Mr Bradford: To use Experian as an example of what we do and the interest in what we do, even without that mandatory requirement over the course of a year we will probably issue 1.5 million credit reports. We will interface with 900,000 to one million consumers. We have a number of leaflets that we ensure are distributed through citizens advice bureaux and so on. The awareness of what we do from that source is phenomenal. I think that people are far more aware than they used to be of what a credit reference agency does. It is not Big Brother where data sits there and there are black lists with all the other very emotive things over which at one point there was concern. We have a strategic imperative in our business to work on consumer education and awareness. I think that we are doing it anyway.

Q165 Mrs Dean: Would you support the idea that there should be a positive way to advise people what is held about them?

Mr Bradford: Obviously, we would without fail support it. All I am saying is that clearly there is already a lot of awareness. We try to go beyond our basic statutory requirements to inform, if they ask, but to take it out there through citizens advice bureaux and working on various government committees, like the Over-indebtedness Task Force and so on, to try to work as a public/private sector partnership to educate consumers in the round about their financial management, not just the bit that sits in a credit bureau. It is a far bigger issue than just a credit bureau; we are just part of it. That is why we try to tackle it very much on a holistic basis.

Q166 Mrs Cryer: Mr Bradford and Mr Sklaroff, do you believe that the constant introduction of new technology is making compliance with data protection regulations more complex or simpler?

Mr Bradford: We operate credit bureaus throughout the world and so see various challenges. Interestingly, the European Data Protection Directive as enacted in the UK under the DPA is very technologically agnostic. The point was made earlier that as technology moved on the same basic data protection principles applied. That is probably one of the strengths of European data protection. We are not overtaken by technology. If one looks at, say, the encryption standards that organisations adopt now—126-bit encryption algorithms, ISO standards and heaven knows what—those have all moved on in the time since the introduction of the Data Protection Act in 1998. If it was very technologically based we would have had iterations and amendments. I think that the fact the Act itself is concerned with very high level key principles means that it can be a piece of dynamic legislation that moves with the times.

Mr Sklaroff: The self-regulatory machinery which sits alongside the statutory machinery is similarly set up with a number of principles which are technology neutral. They are called the principles of reciprocity

and the industry body which looks after them and makes sure that data is shared only for legitimate purposes is charged with ensuring that those principles rather than any particular detailed technological specification are applied.

Q167 Mr Clappison: Following on the question of the legitimate use of data, there is concern about the criminal use of illegally obtained data. Are you confident that your member companies are doing all they can to prevent criminal access to your databases?
Mr Sklaroff: I am confident. Our member companies take this very seriously. No system is ever perfect and more always needs to be done, but it is another area where they have not only a public responsibility to take this very seriously but, picking up an earlier point, a clear commercial interest in taking this matter seriously. Therefore, continual efforts are made on that front and I believe that the situation continues to improve.

Q168 Mr Clappison: You may have heard the earlier witnesses telling us that as far as penalties were concerned they took the view that very strong measures and appropriate penalties needed to be taken to prevent this happening. We hear that various figures including the Information Commissioner have called for tougher penalties. Do you go along with that?
Mr Sklaroff: We have already made public our view that tough penalties are a very important part of the machinery we have to prevent this kind of breach. We are very much in favour of that. The one proviso is the targeting of investigations prior to enforcement. As with any area of regulation, it is important to make sure that the effort is going into the areas of greatest risk among which would be those people who are quite consciously engaging in criminal activity. That is something on which we would like to see greater focus.

Q169 Chairman: Another comment made by the American witnesses this morning was that, criminals being criminals, penalties did not necessarily deter them and the focus should be on punishing the holders of data who allow it to be stolen. They were talking about the responsibility to contact individual customers but also the financial penalties that one could impose on those organisations. In your evidence you have not been keen collectively on being fined for mislaying data. But there is a logic in the US experience, and the thing that will really focus your minds is not just customer trust but the fact that you have to tell customers and pay a financial penalty upfront should you allow a criminal to get hold of the data, whether by accident or design?
Mr Sklaroff: That is absolutely true. Our point is simply that there needs to be a balance because there are many reasons why data in any given instance may have been released in a way it should not be. It is important when talking of enforcement and penalties that those reasons are looked at. It seems to me that there is a difference in principle between a company that is taking its responsibilities very seriously but makes a mistake and corrects it and a company that is quite consciously cavalier.

Q170 Chairman: Mr Bradford, Experian operates internationally in different regulatory regimes?
Mr Bradford: Yes.

Q171 Chairman: Which regime do you think is most effective? Which worries you most in terms of the cost to you if you get things wrong?
Mr Bradford: Those are two different questions. I would argue that the most effective one is the geography that provides our clients, predominantly lenders, and consumers in that country with the best balance of safeguards for data but also the ability to do business as clients and obtain goods and services as consumers. I will embellish that in a minute. If I look at the UK as an example, the World Bank, which is in the news but is fairly independent as an arbiter, rates the UK as one of the best countries, if not the best, in terms of the balance of privacy rights and the ability for data-sharing and so on. I think the UK probably has it right. The Information Commissioner in the UK adopts a very pragmatic stance to the benefit of the individual and the commercial benefits. If I look at other countries, for example Spain, it is altogether different. It has higher penalties not necessarily for data breach but for breaking its data protection legislation. If I look at France, that has a completely different regime which is very consumer-oriented, almost paternalistic. The consumer is perhaps not able to make a decision for himself and so the state must protect. When one has that type of approach to privacy one ends up, unlike the UK which has a very healthy and supportive credit industry, with a different type of regime. I think the most important question is the balance rather than privacy for privacy sake, because privacy should not be viewed in a vacuum; it is there to protect the consumer but also to enable the consumer to obtain goods, services and so on. In our experience, we believe that the UK is probably the perfect example of good balance.

Q172 Mr Benyon: Do you believe that the expression "identity theft" is used as a bit of a cop-out by banks and other organisations to shift responsibility from them onto the state, if you like?
Mr Sklaroff: I do not think so. I think it is taken very seriously as a concept and a problem. For example, the industry I represent is actively engaged in discussions with the Government and others at the moment in setting up an identity theft programme which will help consumers who have suffered that to correct the problems which then ensue. It is a very serious problem which goes to the issue of trust, and the industry is very keen that it be addressed vigorously.
Mr Bradford: I very much support that. Certainly, we are working with the Treasury and trade associations, including Mr Sklaroff, on the initiative that the Government is looking at. We have operated our own victims of fraud service within Experian since 2003. This is a real issue.

Interestingly, we find that a number of consumers believe that their identity has been compromised but it has not. We receive about 100 calls a week from people who believe that a credit card has been compromised or whatever. It is a real issue but something that the public and private sectors should work on together, as we are with the Treasury. It is a collective responsibility.

Q173 Chairman: I want to turn briefly to Tesco and LMG. Obviously, you work very hard to ensure that people understand the direct benefits to consumers of using loyalty cards. How important is it to you in terms of your business practice that the public fully understands the range of uses to which the data is put? If we have one of these cards do we understand the deal for which we are signing up? We understand what we get from you but do we understand what you get from us?
Mr Briggs: There are two aspects to this, a legal and commercial one. The legal one is a requirement under the Data Protection Act to ensure that consumers are absolutely aware before their data is collected as to what that data will be used for, how it will be used and to whom it will be disclosed. Those are the bare bones of the law, if you like, but, much more importantly, if consumers really begin to distrust us and are not happy with the way we use their data they will cease to use our programme. To ensure our continued viability we must not compromise that trust.

Q174 Chairman: Recently, Google announced that it would anonymise its search engine data beyond a two-year period. Mr Eland, did you say that you kept data for two years?
Mr Eland: Yes.[3]

Q175 Chairman: Have you ever thought of saying to the users of your Clubcard that you will anonymise the data or not use it in a much shorter period than two years?
Mr Eland: I would like to make two points. One is that we keep the data as anonymised as possible so we will ring fence it in a way to ensure that as far as possible profiling and so on occurs at an anonymised level. It terms of the amount of time we keep the data, it reflects the amount of time we need to process it. For example, some customers may shop at dot.com once a year at Christmas time, so two years is a reasonable amount of time to understand their shopping pattern and to reflect that. But we always look at retention periods. I think the underlying point from the legislative point of view is that we will ensure we do not hold data longer than necessary. If we are to hold data longer than that wherever possible it is anonymised.

[3] *Note by witness:* We hold full transactional data for Clubcard customers that we use for a maximum of two years.

Q176 Chairman: Mr Bradford, the final question is about profiling which runs throughout our inquiry, for example the use of all sorts of different databases, whether it is to predict which young people will run into trouble with the law or whether it is for the benefit of lenders or whatever. How good is credit profiling now as a real predictor of subsequent human behaviour? I ask the question because one of the issues raised with us is the dangers of profiling, that is, whether it be your organisation or others, to assume that what the profile tells you is a particularly accurate predictor of how somebody may behave. How good is it?
Mr Bradford: To start from the base point, profiling can only ever be as good as the base data that is being used for profiling. Within my own organisation we provide tools to help lenders build their own profiling systems.

Q177 Chairman: How good is that?
Mr Bradford: With that caveat, the UK for many years has been used to risk profiling, by which I mean that Mike Bradford is not a good risk because he has already had some form of default or county court judgment. We have had many years' experience in the UK of refining those score cards. The more important challenge now, which is largely to do with the fact that in the UK we do not have objective income data, is to build profiling around affordability; in other words, Mike Bradford has never been in arrears or had a default or a county court judgment but he has a series of outstanding loans, all of which are performing exceedingly well, but one more type of loan may take him over the edge. That is the tipping point. It is the score cards that we have been developing over the past three or four years which are accurate for what they can do against the data that is there, but in the UK we will have to work against the lack of objective income data which would plug that gap.

Q178 Chairman: What is the danger that you get either a false positive or false negative? You do the profile and say to Mr Bradford that he cannot have a loan, whereas if you have full information about his personal circumstances it is perfectly clear that he can manage it?
Mr Bradford: It is difficult to tell, because with more data now being in credit bureaus there is less likelihood of that happening. But it is the objective piece that is important. What a lender has to do is take the objective, factual and accurate data from the bureau and marry it with, one hopes, the equally factual and accurate data that the applicant has provided. That is the subjective bit of it. One is reliant on two data sources for that decision.
Chairman: Gentlemen, thank you very much.

Tuesday 12 June 2007

Mr John Denham, in the Chair

Mr Richard Benyon	Gwyn Prosser
Ms Karen Buck	Martin Salter
Mrs Ann Cryer	Mr Gary Streeter
Margaret Moran	Mr David Winnick

Witnesses: **Professor Ross Anderson**, Professor of Security Engineering, University of Cambridge, and Chair of the Foundation for Information Policy Research, **Mr Pete Bramhall**, Manager, Privacy and Identity Research, Hewlett-Packard Laboratories, and **Dr Andy Phippen**, Lecturer, School of Computing, Communications & Electronics, University of Plymouth, gave evidence.

Q179 Chairman: Good morning, gentlemen. Thank you very much indeed for coming to give evidence as part of our inquiry into the contention that we are drifting towards the surveillance state, whether that is a good or a bad thing and what we might do about it if it is, and we are grateful to you for coming. Our aim today, as you know, is to get at least some understanding of some of the technological issues involved in these developments and we are very grateful to you for your time. I understand that Caspar Bowden cannot come due to ill-health which is unfortunate, but I am sure that, between you and with the expertise you have got, you will be able to answer the questions that we might have directed to him. Perhaps I could ask each of you to introduce yourselves for the record and then we will make a start.
Professor Anderson: I am Ross Anderson, Professor of security engineering at Cambridge and I also chair the Foundation for Information Policy Research.
Dr Phippen: I am Andy Phippen. I lecture socio-technical studies at the University of Plymouth and am co-author of, amongst other things, the Trustguide Report.
Mr Bramhall: I am Pete Bramhall and I lead a small team of researchers at Hewlett-Packard's corporate research labs in Bristol where we do research on privacy and identity management technologies.

Q180 Mrs Cryer: May I ask the first question primarily to Professor Anderson and it is in terms of surveillance capability. What do you feel has been the most significant technological development of the past 10 years?
Professor Anderson: Almost certainly search engines. It is perhaps slightly more than 10 years since we saw the first one, AltaVista, 11 years ago, but certainly Google has come along in the past six or seven years and their use has become very widespread. Previously, lots of information about people was kept on numerous, disparate databases, and a lot on paper in filing cabinets. Search engines mean that everything that is searchable is now findable if people have got the wit to look for it, and of course there are not merely the publicly available search engines, such as Google; there are search engines on intranets and there are search engines available to government and intelligence services which give access to information which is not generally available to the public. But overall the killer technology is search engines.

Q181 Mrs Cryer: Do you both agree with that?
Mr Bramhall: Yes, I would agree certainly with that and I would perhaps also add the fairly recent rise in social networking capabilities on the Internet, the rise of things like MySpace and YouTube where people can post information about themselves and yes, they are doing it willingly and for what seem to be very desirable purposes for them at the time, although they may actually have cause later in life to regret what they have made available of themselves and, coupled with search engine technology, there might actually be more out there than they would be happy with.

Q182 Mrs Cryer: Dr Phippen, do you go along with that?
Dr Phippen: Yes, I would certainly agree with that.

Q183 Chairman: Can I follow that and ask what the main drivers are of these new technological developments? Search engines and Google are presumably driven by a commercial motive, but things like Facebook and social networking were sort of invented by people out there really, thinking of a way of doing things and making uses of them which probably the original designers had not thought of themselves, so what are the main drivers that are moving technology forward as quickly as it is?
Professor Anderson: I think it is different in the private sector than the public sector. In the private sector, the main driver is the wish to charge different people different prices. This is of course as old as people have been trading; the carpet trader in Istanbul who makes a special price "just for you" is the price discrimination of antiquity. In general, price discrimination is economically efficient, but people tend to resent it because they feel that it is unfair. Now, what is happening is that technology is making price discrimination, firstly, more attractive to businesses because businesses become more like the software business over time and, secondly, easier. So this creates a circle—a vicious circle or a virtuous circle depending on your point of view—which drives the acquisition of ever more data and ever more capabilities as part of the process. And a second main driver of course is targeted communications. In the public sector, we have got all the motivations that we have all come to know and love or hate, as may be the case.

Q184 Chairman: Could you say a little more about the public sector motivations though in the sense that there is probably a similar desire to get the right piece of information to somebody or the right service to somebody or the right information about somebody, so is it significantly different and is the public sector driving the technology or is in fact the private sector developing the technology which the public sector makes use of?
Professor Anderson: I think it is the latter. The UK is rather odd in that over the last few years a majority of the business won by our big systems houses has been public sector business rather than private sector business, but they are almost never developing new technology, they are simply using technology which has been developed mostly elsewhere for private-sector purposes. It is also difficult for even a mild cynic to escape the supposition that there is some competitive empire-building going on in Whitehall of the "my database is bigger than your database" variety, and this appears to be more pronounced in Britain than in other countries.

Q185 Chairman: Mr Bramhall, as you mentioned it, how significant are these social networking initiatives in driving change? I suppose it goes back certainly to text messaging originally, things where consumers have invented ways of using these systems that people had not previously thought of.
Mr Bramhall: Yes, the technology behind them, I think, tends to come from private sector considerations. Entrepreneurs will think, "Ah yes, if I set up a capability of doing a MySpace or a YouTube, then they will come and use it and it will be commercially successful", but the other factor that drives that success, or otherwise, is essentially how great is the take-up by people. Are they actually as popular as the entrepreneurs who found them would like them to be? We can all look at the numbers of how quickly those sites are mushrooming and so on, but there is perhaps a little bit of evidence that indicates younger people are more happy and willing to participate in them and, therefore, perhaps one of the drivers is actually coming from the youthful recognition or the recognition by the young that technology is definitely not to be feared, it can do wonderful things, it can be liberating from an individual point of view, it can help form all sorts of personal relationships which again are very important when you are young, and perhaps those are the sorts of drivers of behaviour that lead to the success of these systems which have been enabled initially by private sector technology.

Q186 Chairman: It is probably an impossible question, but, if we looked over the next 10 years, what are the technological developments that you think would have the most impact on data security and on the privacy of citizens?
Professor Anderson: I do not think that privacy is fundamentally a technological issue, but fundamentally a policy issue. One of the things that we have learnt over the past six or seven years is that, when systems fail, they largely do so because incentives are misaligned and classically because some of the persons who guard a system are not the persons who bear the full economic costs of failure. One of the things that we are seeing more and more is that, as systems become more complex with more players, so the temptation on players to throw the risk over the fence and make it somebody else's problem becomes pervasive. So I can see this necessarily leading to an increase in regulation and public action of various kinds. As far as the technology is concerned, what we are going to see is probably a move to a world in which more and more objects are a little bit like computers. In 10 years' time, most things that you buy for more than about a tenner and which you do not eat or drink will have got some kind of CPU and communications in them and even things that you buy to eat or drink may have RFID tags on them.

Q187 Chairman: At which point, the Committee then goes "What?", so CPU and what was the other thing?
Professor Anderson: Some processing capability and some communications capability. Fifty or sixty years ago, there were a handful of computers and now we have several computers on our person, mobile phones, laptops, iPods, et cetera, and that will go up from a few to dozens. Your car might now have 30 computers in it and it might have 100 in it within 10 years' time and many of these computers will talk to each other. What that is going to mean is that more and more businesses will become a little bit like the software business and that means that the problems that we see in the software business, of which surveillance is only one, are going to become more pervasive. And this is going to affect, I think, the work of many committees, because many of the laws and regulations that we worked out during the 20th Century with, if you like, atomic property are going to have to be reworked with digital property to deal with all its side-effects.

Q188 Chairman: Dr Phippen, any star-gazing?
Dr Phippen: I must admit, I am certainly not as much of a technologist as the other two and, just looking from the citizen perspective which is very much where I focus, I think what you realise in the last couple of years is that the age of the naïve user is pretty much over now. We have spoken to people who had never used a computer before who told us, "You shouldn't buy things on the Internet because the hackers will steal your credit card details", so that is the level of awareness you are now dealing with. On top of that, going back to the previous question about whether citizens drive technology, there is a certain element of narcissism, I guess you would say, with blogging and MySpace and things like that where people like to share their information and certainly with younger people that is very prevalent at the moment. However, what you have not currently got, particularly with young people, is that, whilst they are very comfortable with the veneer of the technology, they are not aware of the threat and they are not aware of the long-term

damage, such as when you are going for an interview in 10 years' time and someone pulls up you're MySpace page and says, "If you had said that you paid this political party, would you like to elaborate on that?" because what they do not realise is that this stuff stays for ever, especially with Google caches, and you have got various Internet archive sites that collect websites on a regular basis. I think the citizen perception will increase a great deal, but what I do not see increasing is the awareness of threats from it. Certainly we did quite a lot of work with around 100 school kids and they were very comfortable with technology and actually, since MySpace got bought by Rupert Murdoch, it seems to be a little less cool than it used to be and now things like Facebook and Bebo are the ones to go for, but they are very aware of that and they are very comfortable using MSN and various other messaging technologies and they are very comfortable using SMS technology, but, when you ask them about the threats and you ask them about the potential for stalking and the potential for viruses, they have very little in-depth information.

Q189 Chairman: We will come back to some of those points. Mr Bramhall, just on the technology side, do you have anything to add to what Professor Anderson and Dr Phippen have said about new developments?
Mr Bramhall: Not particularly. I think that in general the technological developments which will come about will still basically be in a context where the privacy issues remain the same and the principles for how one should address those privacy issues will also remain the same. The challenge would be, I think, when one is a system designer, remembering to take account of those principles and not just getting captivated and dazzled by the potential of what the technology could do.

Q190 Mr Streeter: In relation to the last 10 years, have there been any surprises? Actually I sometimes have a bit of a theory that things do not change quite as rapidly as we think they do, but we can see it going from a long way down, so have there been any dramatic surprises where in the next 10 years we might look forward and say that we might have some more like that?
Dr Phippen: I certainly think that SMS technology was not created for kids to bounce messages on to their mates; it was created for engineers to send short messages about mobile network updates. I think there is an awful lot of, if you like, accidental adoption that goes on where people do things in a way that perhaps the creator of the technology did not think.

Q191 Mr Streeter: So a surprise in implementation, not necessarily in the technology or the invention itself?
Dr Phippen: Yes, certainly from the perspective I come from, it is really the use and abuse of the technology in unpredictable ways that is the difficult thing to foresee.

Q192 Chairman: It is almost inevitable that this sort of inquiry moves quite quickly into the threats, the risks and the dangers of the world that we are moving into and I suspect that this session will be no different when we go through the questions, so just before we do, can I just ask each of you to look at the other side of the equation. If we look 10 years ahead with the development of these technologies and the spread of these technologies in lots of different systems, how would you assess the benefits that are likely to arise from them, particularly for individuals, and would you think that those benefits are going to be more evident in the public sector or in the private sector?
Professor Anderson: Well, 10 years ago the big issue was cryptography policy—the US Government's attempt to ensure that nobody communicated privately on the Internet without the NSA being able to tap the communications. That concern has gone away because encryption has not, as a matter of empirical practice, been widely deployed. Apart from that, 10 years ago people were generally very positive about the effects of the Internet. The evidence that we have now 10 years later? The most recent study of the correlation, for example, between crime and Internet adoption across the 50 US states, is interesting. It shows that, by and large, the Internet has a positive effect or a beneficial effect in that it reduces some crimes, crimes of sexual violence and crimes of prostitution, and this is assumed to be linked with the increasing availability of pornography to young males. The only crime that has gone up is what the FBI classes as 'runaways', that is, children leaving home without their parents' consent before age 18. Some cases of runaways are clearly tragic, and others are clearly beneficial to the child, and we have no further figures on that. The things that we were worried about 10 years ago and the things that have happened 10 years after that were different, so we have to be cautious when we gaze into the future.

Q193 Chairman: But would you say that there are more benefits to be gained from the spread of computers and communications?
Professor Anderson: Absolutely, otherwise there would not be such an enormous effort and expenditure going into developing the technology. There are some downsides of course, but the gains are very much greater than the losses.
Mr Bramhall: The benefits being the use at low cost, of the removal of physical barriers or of physical distances being a barrier for communication, collaboration and so on. Those are clearly the benefits and I see those continuing to evolve. The threat is sort of the other side of the coin simply that, because you are able to get out to the entire world from your house, so the entire world can get into you by the same mechanism.

Q194 Chairman: We touched earlier on the sense that possibly the public sector tends to follow the developments in the private sector in this area. Do

you see it over the next 10 years being primarily in the private sector and individuals' interaction with the private sector and with other individuals that the benefits will accrue or do you see significant benefits to the public sector?

Mr Bramhall: I think there is the potential for significant benefits for the public sector because the same kinds of points that were made about ease of use and ease of access and so on are all essentially efficiency benefits and enabling benefits which are possible just as much in terms of public sector internal operations as well as public sector delivery of services to individuals, so those benefits are still equally applicable.

Q195 Mr Winnick: Could I put this point to you, namely that virtually everyone, I would imagine, except Luddites, welcomes the new technology for all kinds of reasons, the computer, the Internet. Certainly my secretary finds that a correction, which otherwise on a typewriter would have taken so long, on a computer takes a matter of seconds. Is there any way in which you feel, gentlemen, that you can have this advance in technology, considerable advance in the last 10 or 15 years, and certainly when I came back here in 1979 the first item I bought was a typewriter, so can we have this advance in technology without the intrusion and growing intrusion into privacy? What about you, Professor Anderson, do you have great concerns about safeguards over privacy?

Professor Anderson: Well, privacy intrusions generally stem from the abuse of authorised access by insiders or from failures to regulate such access properly, so privacy is largely a policy matter rather than a technology matter. That said, however, when you have got order of magnitude reductions in the costs of collecting data, or storing it and indexing it, of course more information is going to be kept, and over time we will move to some new equilibrium which is either going to have to involve more tolerance or more regulation or both. And I expect that the balance will be different on different sides of the Atlantic.

Q196 Mr Winnick: Mr Bramhall?

Mr Bramhall: I take a slightly different view as to the effect. Certainly the policy framework has to be got right and absolutely so regarding privacy and the management of it and so on, but I think there is also the potential certainly in the private sector for companies to differentiate themselves by exemplary privacy practices and to get, if you like, a good reputation as being able to manage the personal data of their customers, employees, whatever, in a reliable and privacy-friendly manner and to pay continual attention to this. I think it could become one of those differentiators between companies in the same way as, for example, product quality might be or price of products, so I think it could become a differentiator, particularly as far as the provision of digital services is concerned.

Q197 Mr Winnick: There is a growing tendency for people to put a great deal of personal information on social networking sites which we all know about, although I do not myself do so, MySpace, Facebook. Is there not a danger that people are doing this without recognising the dangers involved in storing up such personal information and is there any way that we in Parliament or the media can warn people of the dangers involved? Just as a matter of interest, have any of you three put up such information?

Dr Phippen: I do not have a MySpace account and I do not blog, I must admit, but I am planning on blogging about one specific topic I research on. I think there is a massive issue in particularly what the youth are currently doing with technology and the fact that they are nowhere near well enough aware of the damage that can come from that. We did an awful lot of work with awareness and education, who is responsible, and it always comes back when you talk to citizens that it is the Government and it is the manufacturers that should be responsible. For some reason, you always get the car analogies, "I wouldn't buy a car and drive it off and then crash it into a wall because they hadn't checked the brakes properly, so why aren't we checking that computers are secure before they sell them to us?" Now, obviously the trouble with that analogy is that, as soon as you connect your computer at home and stick it on line, all sorts of things that the vendor could not possibly have predicted when they sold it to you might happen. Just as an interesting aside, we do a regular experiment where we get a student to drive around Plymouth and detect available wireless networks and generally every year, up until two years ago, it was always 40% secure and 60% unsecure. Last year, we expanded it out to a few other cities in the South West and it was still 40% secure. This year, it was 75% secure. We then expanded it out, did rural towns, did some market towns and further afield, and it was coming in at around 75% secure. But then, when you start to look down the network descriptions, it is the fact that the vendors are now providing out of the box some level of security, and Professor Anderson will undoubtedly tell you far more than I can about the difference between WEP and WPA encryptions and the relative merits of them. What we are kind of seeing there is that manufacturers are trying to do more, but then there is a separate experiment where we had a student detect unsecure Bluetooth devices and send them an unsolicited message. Over 60% of the people that did that were perfectly happy to receive that on their device and load it up with no problem at all, so the kind of conclusion you are getting from that is that the buck has got to stop with the individual because manufacturers can do a lot, the Government can do a lot by education and I would certainly say that if you looked at School Curricula, et cetera, it is not doing enough at the moment. However, there has to be personal responsibility because ultimately it is a personal device. The bewildering thing we found was that people were very, very willing to accept that

something is in their personal device, they did not know what it was, they just accepted it. Now, how could a manufacturer protect against that?

Q198 Mr Winnick: I take it, Professor Anderson and Mr Bramhall, you do not put anything on these sites which I mentioned?
Professor Anderson: I have a MySpace site, but I basically use it for one of my hobbies, old music. It is a free repository for out-of-copyright MP3 files and things like that. On the issue of security usability, this is one of the hottest topics in security research over the last three years because of the rise in phishing and other attacks that basically exploit user naivety. Up until now, many of the organisations which ought to know better have taken the view which in safety-critical systems we call 'blame and train'. If somebody cannot use your system, you first blame them and you then make some half-hearted effort to train them. Now, that is known not to work in safety-critical systems. If an aircraft cockpit is unflyable, you redesign the cockpit, for goodness' sake! You do not try and make the pilot fly in some strange attitude, and we are going to need a similar change of attitude among banks, for example, whose websites are often particularly vulnerable. There are some interesting public policy issues here and one that we have been looking at recently is what is known as 'gender HCI', the way in which men and women interact with human computer interfaces differently, and this is a subject which started only in the last year or so at Cambridge and Carnegie Mellon. We are beginning to realise that the way many bank websites are designed, for example, likely discriminates against women because they are designed by geeks for geeks. Banks will say things like, "visually parse the URL and look for the second-last thing before the last slash", and this is a boy-toy kind of approach to things. In such sectors, there are a number of suppliers—not just computer suppliers but also website operators—who really must do better. So this is an active area of research.

Q199 Chairman: I did not want to say this because, as Dr Phippen says, we always seem to get car analogies and I was sitting here with a car analogy! Professor Anderson, as you were saying earlier, most of the breaches are about when people get inside the system rather than the technology, but it does sound like the argument that it is not cars that kill people, it is car drivers, but actually in practice we have done a lot to make cars people-proof over the years because you could not just blame the driver, you actually had to change the design.
Professor Anderson: Well, these are complex socio-technical systems and the reason that we have got about the same number of fatal road traffic accidents now as in 1925, despite having a couple of dozen times more cars, is due to a whole lot of factors: that cars have seatbelts, they have crumple zones, we have speed limits and we enforce them, drunk-driving is no longer socially acceptable, et cetera, et cetera, et cetera. And do not discount the long evolutionary period whereby the Department for Transport looks at the road traffic accident hot-spots and, if two or three people have been killed at some particular interchange, they redesign it. There is a long period of growth, learning and adaptation which has gone behind this reduction in fatalities.

Q200 Mr Winnick: Arising from what you have just been telling us, Professor Anderson, do you feel that large retail stores, banks, insurance societies and so on are asking for too much personal information when it comes to various matters like loyalty cards, travelcards and purchasing items on the Internet? Are they going over the limit as far as personal information that is being requested is concerned?
Professor Anderson: Sometimes too much information is requested and sometimes too little, and it depends on the application because surveillance is, after all, about power and it is part of another system, namely the way in which organisations, be they governmental or large private sector organisations, exercise various kinds of power, market power or otherwise. Now, generally, organisations err on the side of collecting too much information simply because it is cheap and it does not cost you very much extra to have an extra computer disk drive or two to hold more information about individuals and, if it is their time that is spent filling out the web form rather than your staff's time, then the marginal cost to your organisation is very low. Now, where things are competitive, there will be limits on that because, if your website is too much of a bother for people to fill out, people will go to other websites. But there may ultimately be a need for systemic controls on the amount of information gathered by public sector bodies or others who are not subject to competitive pressures. America some time ago had a regulation about the maximum amount of time that people would have to spend filling out government forms with the requirement that these actually be tested, and perhaps we will need something similar in the future here.

Q201 Mr Winnick: Arising from what the Chairman said, Mr Bramhall, should people be more concerned that the private sector have information on them equal or perhaps even more than the State have? Generally, people are not too worried, at least in a democracy, which we can emphasise time and time again, about the information that social security departments and so on have on individuals for very obvious reasons, and the Health Department, but is there less confidence when it comes to the private sector?
Mr Bramhall: Yes, and again there is a wide variety of practices and I am certainly not going to tar all the private sector with the same brush, but it is not too difficult to find instances where you do feel, as you are interacting with a private sector website, that perhaps it is not only asking more information than is really needed for the purpose that you are interacting with it for, but they might have a different purpose, and increasingly as technology, particularly privacy-enhancing technology, begins to offer possibilities for system designers to design

the systems in a way that actually requires less personal information, then I think the incentive to them to do so is not actually apparent at the moment because they are sort of stuck in this habit of gathering more information because it might come in useful some day. I am not going to sort of point fingers or, as I say, tar the whole of the private sector with all of the same brush there, but there are concerns and I think some of those concerns are valid simply because having too much information and having information that is not strictly needed for the purpose runs the risk of leakage, runs the risk of loss and runs the risk of it being found by people who should not find it. In fact, in many of the data breaches that one reads about where personal data is disclosed from an organisation that had a valid reason for keeping it, it is quite often just a sort of failure of practice and perhaps incompetence even at a fairly low level that just allows it to happen, so there is an opportunity for a better job to be done definitely so, but it is not unremittingly awful or anything like that. As I say, most organisations really want to do a good job with handling personal data, public sector and private sector, and they certainly do not wish to risk the opprobrium that comes with the bad publicity surrounding a leak.

Q202 Margaret Moran: Could I just pick up on something Professor Anderson said, and let us not mention DWP in that last context! I was very interested in the comment you were making about recent studies in relation to the gender differential in the ways that technology is used and, therefore, the way that people approach the privacy and security issues. You may be aware that six or seven years ago there was a report called *Code Red* by Perri 6 of IPPR, and I actually wrote something called "He Democracy or She Democracy" which looked at the codes behind the software, so we are not actually talking about the car, we are talking about, I guess, the spaghetti in the car, all the electrics in there. The way that codes are used within systems that we all use, whether it is a computer or a hand-held, the way that they are devised actually leads us to a certain form of encryption and security and that is very male-dominated, as you said, the geeks, as we traditionally like to think, in the bedrooms. How far do you think that recognition is helpful in identifying more secure forms of data-sharing and the use of the services that we all want to use in a safer way? How far is that developing?
Professor Anderson: I think we are at the very early days of gender HCI. Work started a couple of years ago at Carnegie Mellon[1] looking basically at how you could redesign programmers' toolkits so as to make it easier for women to be programmers. We have been looking at the effects of this on security and, in particular, vulnerability to phishing. Talking about it to a few people over the last few months, it seems there is interest sparking elsewhere and it is the sort of thing I would expect to see more papers on over the next few years and conferences. There are of course a number of established IT policy issues that bear on women, and someone mentioned the children's databases, for example, and there are also supermarket loyalty cards where the majority of these are held by or at least substantially used by women. It would be a large task to pull together all the women's issues in this space and, if your colleagues are interested in getting involved in that, then I would welcome it.

Q203 Margaret Moran: Going on to the PETs, privacy-enchancing technologies, the essence of what you have been saying really is that this is the way forward in terms of being able to deliver what we want, but at the safety level that we require. You will know about the growth of PETs and the idea of the token that Credentica has developed. How far do you think that these systems can be really designed for privacy? With things like data-matching, and people have criticised iris tests, biometric tests, there is a very lively debate on that one, the authentication techniques are getting a lot better and becoming more accurate, but do you think we are getting there in terms of surveillance and can we go further?
Mr Bramhall: Are we talking about surveillance or protection against surveillance?

Q204 Margaret Moran: Protection against surveillance.
Professor Anderson: Well, I think you will find differing views on this from different witnesses. I was involved in the 1990s in developing a number of what would now be called 'privacy-enhancing technologies', and I invented the steganographic file system, for example. In recent years, I have become somewhat of a sceptic because, to a first approximation, privacy-enhancing technologies are just pseudonyms. They can be dressed up in various fancy ways, but at heart they are pseudonyms. There are many circumstances in which it is very, very sensible for people to use pseudonyms and, in particular, teenagers going online and having pages on Facebook or whatever are well advised to use pseudonyms for fairly obvious reasons—everything from personal safety to not being embarrassed in 25 years' time when they are trying to get themselves elected as Prime Minister—but there is only so much you can do with pseudonyms. Companies do not want to deal with pseudonymous individuals, by and large, unless there is some premium in it for them. You can get prepaid credit cards, but they are significantly more expensive and the reason for this is that the information that is collected about you is valuable and it is used for price discrimination. So there are some market niches for privacy-enhancing technologies, but they are by no means the general solution to surveillance problems.
Mr Bramhall: I would actually take a slightly different view on that one and it stems from perhaps a broader definition of what are privacy-enhancing technologies, and I do not agree that they are just pseudonyms; there is a wider set of technologies that can be used. There is quite a useful definition of them in a communication which the European Commission has published recently on this subject

[1] *Note by witness:* I was mistaken—the earliest work was at the University of Oregon. See http://eusconsortium.org/gender/

and it takes a definition as being a "coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system". That then opens up a wider range of possibilities. Certainly what you might regard as the more mathematically rigorous and tighter sets of technologies are the pseudonyms and similar that Professor Anderson refers to, but there are other models by which personal data can be managed or its use be reduced. There are other models which are more to do with helping the organisation that has got that information, that has actually received personal information, helping it do a better job of managing that information, of controlling it, and putting processes in place which design the systems that do those things.[2] Those processes are as much to do with management practice as they are to do with technology and, by themselves, those processes require some technology to help them as well, so I would actually take a wider definition of what constitutes a privacy-enhancing technology. I agree with Professor Anderson's point that, if everyone just takes pseudonymity as a starting point, the incentives there are not very strong for an organisation to pick that up, but there are other technologies too and, as I have already made the point, I believe that privacy can be a differentiator for an organisation.

Q205 Margaret Moran: We have heard evidence from the Royal Academy of Engineering that personal identity will offer the sort of security that people are looking for and they have also said essentially that, if we were better at encrypting and more sophisticated in terms of our encryption, then some of the concerns we are discussing here today would not occur. How far do you agree with that?
Mr Bramhall: I suspect it actually comes back to Dr Phippen's area which is ways of making it usable. I think the basic encryption technology could be made strong enough, et cetera, but the question then becomes how do you make that usable and accessible and to the ordinary person, I would guess.
Dr Phippen: Yes, certainly if you say to an individual, "Use this site, it's got better encryption than before", they are going to go, "So what!" The public's view of encryption is whether the little padlock is on the browser and, if the padlock is on the browser, it is safe. I think the usability issues are extremely significant if you are looking at privacy-enhancing technologies at all and, unless your average person on the street is comfortable with them, guarantees of security will be ignored in a lot of the cases. We generally started our discussions with, "Who do you trust to keep secure information about you?" "Well, there is no such thing as a secure system", is generally the response coming back. "Well, how do you know that?" "Because we've read about it", "Because we've got friends who've got it", "We've had peers that have experienced it", or "I've experienced it myself". "Well, why do you use these things then?" "Convenience, I guess". I do not think security is the big issue, but it depends where you are coming from. If you are looking to get more people online and looking to get more people using public services online, I do not think security and privacy are the issues; I think convenience and education are the issues. You will be amazed at how much personal information someone will give you if you offer them 50 quid off a washing machine or something like that. I guess with a lot of public sector information is that it kind of goes into the, "What's in it for me?" mentality to the individual. If you are buying something online and you are saving yourself 50 quid, it is very clear. There are some very successful public sector e-delivery mechanisms, such as the DVLA and tax returns, and school admissions systems for some reason are incredibly popular because they offer a sort of return in terms of convenience to individuals and they are not saying, "I'm not using that" because you are not using the most up-to-date encryption mechanisms on it, but they are saying, "I'll use that because it will save me having to fill out the form on paper or it saves me having to phone someone up and do it all on the phone".

Q206 Margaret Moran: We have heard from the Surveillance Studies Network that PETs will, or could, lead, as you were saying, to a division within the market and there could be a situation where those who can afford it will have an enhanced level of privacy or, conversely, a lower level of surveillance, whichever way you care to look at it, and that what could be happening through PETs would be a privacy divide where the well-off can protect themselves and have the e-castles around them, if you like, and the rest are without drawbridges. How would you argue that?
Professor Anderson: There are possibly two different issues here. When it comes to the private sector which is interested in price discrimination, anybody who earns significantly above the national average should logically have an incentive to invest in privacy technology, although this may not be technology so much as using pseudonyms, deleting your browser cookies from time to time and so on and so forth, and all of these techniques will eventually become known to people. In the public sector of course there are issues, such as the children's databases where the idea is to gather information from health, schools, social work, et cetera, about children who might be at risk of offending. And the great problem there, as was pointed out in a report that we wrote for the Information Commissioner, is stigmatisation. Equality activists used to joke about the emotional offence of 'Driving while black' and, if we end up with an offence of 'Driving while having more than 50 points on the Home Office's ONSET database', then that would be an equally bad state of affairs. These issues perhaps give some insight into why the State will have more incentive to do more surveillance on the poor and why the rich will have

[2] *Note by witness:* Processes which improve the design of these systems.

more incentive to escape such surveillance as can be conveniently escaped—because they do not want to be charged more for their airline tickets.

Mr Bramhall: I think the actual cost of an individual adopting a privacy-enhanced approach to what they do is probably not the issue. I do not think from an individual point of view that using a privacy-enhanced approach to their interactions is going to have a cost impact at all. I think, however, there is a difference between cost and price and the issue then becomes whether the providers of digital services would wish to price perhaps discriminatorily such that the privacy-sensitive services are at a higher price than the other ones. I think then perhaps it becomes a question for society as to how much it is willing to countenance the possibility of a privacy divide, as you described it.

Q207 Chairman: I am struggling here a bit about the emphasis that goes on to individuals because we seem to be getting evidence that says there are systems that you can do now which give a very high level of privacy protection to individuals. Not in every case, but in many of the cases that we are worried about, which is when we are doing financial transactions and things of that sort, those are generally backed up by the use of one of a handful of major credit card organisations. I do not see why it is so difficult to imagine a situation where you have persuaded Mastercard and the rest that they would not accept transactions through websites which did not automatically build in that level of individual protection. We seem to be in the sort of Stone-Age level of debates about what we can expect from the private sector here. It is rather like the old mobile phone debate and the difficulty in getting mobile phone companies to knock the phones off their network when they have been stolen, even though the technology to do that is cheap and available, but they just cannot be bothered. When we keep saying that the individual has got to be persuaded that this is worthwhile, is it not the truth that we are just not making sufficiently strong demands on a small number of quite strategic organisations, particularly credit card companies, which could basically wipe out the websites that did not have high levels of privacy by just saying, "We're not going to accept financial transactions"? I have not really understood, unless there is something basic that I have missed here, why it is so difficult to get that.

Professor Anderson: I do not think that particular approach will work. There have been so far a couple of competition inquiries in the UK which found that the business of acquiring credit card transactions was anti-competitive. Mastercard would not get involved. One of the things that has been brought about by the dotcom boom is that it is now easier, if you are a merchant, to get credit card transactions processed and that has been of enormous benefit to the economy. The real problem here is a consumer issue, namely that in the UK disputed transactions between cardholders and credit card companies and indeed between credit card companies and merchants are not properly regulated; the banks have got too much power in the regulatory system and are too good at dumping costs on cardholders and merchants. Now, I know that is really the ambit of another committee, but, if the members care to watch *Newsnight* tonight, there is a programme on precisely this topic, so yes, regulatory action would be a good thing, but it is regulatory action that the Financial Services Authority should be taking—

Q208 Chairman: Absolutely, yes, that is what I am getting at, but it seems to me that, of all the transactions we are worried about, they are actually processed in practice by a relatively small number of strategic companies globally and actually, if you could in some way put the squeeze on them over the way they did these things, we could speed up the intellectual privacy technology.

Professor Anderson: I have argued for the squeeze being put on banks in front of a number of committees over the years, most recently the Lords' Science and Technology Committee in March.

Chairman: Well, we will have a look at their evidence.

Q209 Margaret Moran: I think if Caspar Bowden were here, not speaking within that term, I think he might have a different view from that, so we can ask for his view, and of course the RIPA debate was pretty well all about this as well. Just looking into the future, can you anticipate, or what would you anticipate are, the forthcoming technologies beyond those which we have already discussed which would influence the way that people maintain, protect and use their digital identities? What is it that is coming onstream that might offer us that comfort and will any of it overcome what appears to be a worrying privacy divide that we just touched on?

Professor Anderson: Well, I suppose I might take issue with the concept of a digital identity. I know that there is a great push in government—specifically from the Cabinet Secretary—to embrace the whole idea of identity management. But this was something which was tried in the private sector in the late 1990s by companies like Verisign and Baltimore, and Verisign survived by getting into a different business and Baltimore went bust, taking £23 billion of pension fund money with it. I do not think that identity management is the right way of thinking about these things. Instead, one should think about the underlying business process of people, when they go to a government office, being dealt with in a fair and reasonable way; whether banks' transactions with their customers are regulated reasonably. The reason for this is that the rhetoric of identity becomes a means of passing the buck. In the old days, if someone went to the Midland Bank, pretended to be me and borrowed £10,000, that was impersonation and it was the bank's fault. Now, it is my identity that has been stolen, so it is supposedly my fault, and I end up having a furious row with the credit reference agencies. So the construction of the concept of 'identity' as something that belongs to me, that I have to protect with the help of government is not particularly helpful in this debate.

Mr Bramhall: I do not think there is going to be sort of a strongly technology-oriented answer to that question about providing the security and the feelings of security and privacy that people are looking for. I do not think the issue is fundamentally one of the technology and its capability of addressing that issue; I think it is much more about education and awareness and people following good practice and, by that, I do not just mean the individual, but system designers following good practice. Admittedly, that good practice should, where appropriate, use the best and most appropriate technology for the purpose, which might be stronger technology or weaker technology, but it should be fit for purpose, and I think a lot of the issues then revolve around making it clear where information can be readily found as part of that education process,[3] what kind of restitution can be given for where things go wrong[4] and so on, those kinds of things acting as the incentives for affecting the behaviour of both the system designers and the individuals.

Q210 Margaret Moran: Do you agree with Professor Anderson about the regulation of banks? I chair an organisation called EURIM[5] which deals with IT issues which has been arguing to slap an assurance badge on the banks or the credit regulators for some time because it is impossible otherwise to police this whole area of e-crime and so on. Do you agree with that?

Dr Phippen: Yes. Certainly it has been an interesting 12 months for banks because, when we did our initial studies, people would trust banks more than anything else, but, because of the bank charges in particular being very high profile, banks have come in for a bit of a bashing as far as public perception is concerned now and yes, I would certainly agree that they need reining in.

Mr Bramhall: I think, where appropriate, because regulation is obviously the stick, we should not forget to look at the carrot as a way of influencing behaviour as well.

Q211 Mr Winnick: On identity theft, Professor Anderson, you give an illustration that in the Midlands Bank, and I do not know why you put the Midlands Bank, but be that as it may, a good identification, it used to be called, if some money was stolen by criminals, then it was the bank's fault, impersonation. Now, the argument of such financial institutions is that it is identity theft and the responsibility is put on the individual. Should companies not take more precautions to guard against such loss?

Professor Anderson: Well, again this comes down to economics. Now, in the old days, a bank, the Midland Bank of yore or whoever, could decide how vigorously it was going to investigate the background and identity of people who opened accounts with it and every so often they would take hits and that was the cost of doing business. Now, if they can externalise, if they can transfer out some of the costs of that fraud, then the balance point in their business will be different, in other words, they will become more careless. There are further problems in the banking sector in particular with the move to identity as the great buzzword of progress. I was commissioned to do some research for the Federal Reserve Bank a few months ago basically into technological aspects of phishing, fraud and money-laundering. They were interested in non-banks and organisations like eGold and so on and how this fits in. One of the things that we found was that the increasing emphasis on identity since 9/11, that is, asking everybody who opens a bank account for a couple of gas bills, had been at the expense of more effective controls, because knowing the customer and following the money are not perfect substitutes. Providing that banks can consider that they have discharged their duty by having a couple of copies of gas bills in a filing cabinet, they then feel able to be more careless about perhaps more important issues about the conduct of the account—about whether it is being used to send money to dodgy places and about other things that can go wrong. So for a number of reasons one has to be very careful with this whole identity gospel that is being preached. I know it is fashionable, but that does not make it right.

Q212 Mr Winnick: Without wishing in any way to raise the blood pressure of the Chair, you make the point that dealing with identity theft as a description helps the Home Office to sell identity cards to the public. I agree with you as a matter of fact, but what evidence do you have for that?

Professor Anderson: The Home Office produced a couple of briefing documents a couple of years ago detailing identity theft and saying that identity cards would help to stop this. Lumped in with identity theft, they had all sorts of crimes of impersonation and they also appeared to include pretty well all the UK's credit card fraud. This was discussed extensively at the time and I believe I testified to this Committee in 2004 on the subject. It is clear that the banks saw this as a convenient bandwagon and hitched their liability management campaign to it.

Q213 Mr Winnick: Do you agree with that, Dr Phippen and Mr Bramhall?

Dr Phippen: Yes, I certainly agree with it.

Mr Bramhall: I think there is a role for strong identity in some aspects of people's lives, but, I agree with Professor Anderson, having a strong identity is not the answer to all the problems.

Dr Phippen: I think one issue is the concept of a single online identity. I think citizens are very comfortable with multiple identities for multiple things and the Varney Report and things like that are talking about a single signing for all government services and things. The question you get from citizens is, "Why?"

[3] *Note by witness:* Making it clear to both the individual user and the system designer.
[4] Note by witness: Restitution for individual users.
[5] European Information Society Group.

Q214 Mr Winnick: Would you say that security technology in general is keeping pace with the innovation of criminals?
Professor Anderson: It is a constant co-evolution. The most recent innovations in crime have not been principally technological, but principally psychological because, as the technology gets better, so it becomes easier to deceive individuals, so we are seeing an enormous rise in phishing, in pretexting and other things that involve deceiving people. The criminals are not going to stop deceiving machines as well and we are going to see keystroke loggers, we are going to see the rise in pharming and we are going to see technical crimes going along with crimes that involve deceiving people.

Q215 Mr Winnick: Do you feel that, when identity cards come about, the more sophisticated type of criminal gangs will be able to do a pretty good impersonation of such cards?
Professor Anderson: I do not think identity cards are particularly relevant to online concerns because, like it or not, online technology is designed and built in America and companies like Google, Microsoft and Yahoo could not care less about whether Britain has identity cards or not. There are one or two countries, like Estonia, who have tried to issue national identity cards that are linked to a capability to transact online, but this does not seem to have taken off because from a technical point of view, if you want to use client SSL certificates in your banking system, you can do so anyway. Banks decide not to do that for their own reasons, so for governments to make freely available something that is already freely available in another context is unlikely to change very much.

Q216 Mr Benyon: Mr Winnick has cleverly asked most of my questions. I wonder if there are any other drivers behind developments in security engineering that we should be aware of.
Professor Anderson: The two big drivers in security engineering recently have been, firstly, digital rights management and, secondly, Trusted Computing. Digital rights management was driven by the desire of the record companies, as they saw it, to stop people stealing music by sharing it. It has backfired on them rather spectacularly because it has moved power in the supply chain from the big record companies to online distributors, such as Apple. This has happened just in the last two years, so by calling for better digital rights management, the music industry basically destabilised itself and may have handed power in this industry to others. The other great driver in security technology has been Trusted Computing which was an attempt by certain large American technology companies to lock its customers ever more tightly into its products. This is linked with rights management in that Microsoft appears to be trying to gain a worldwide lead in the distribution of high-definition digital video just as Apple has got a lead in the distribution of digital music. It appears to be running into trouble in that Microsoft is having great difficulty in making the technology work. These have both been technology-push drivers pushed by particular industrial interests. As with customer pull, the fundamental problem in privacy economics is that, although people say that they value privacy, they behave differently. This is really the elephant in the living room as far as those of us who study the subject are concerned. My own view, for what it is worth, is that it is a matter of delayed reaction among other things in that the technical and political elites have understood for some time that privacy is an issue. That will percolate down to the man on the Clapham omnibus once we have seen a few suitable horror stories in red-top newspapers. We see signs of it starting.

Q217 Mr Benyon: You have spoken about the difference in approach on each side of the Atlantic. How does the UK compare with other countries in general in safeguarding digital identities and preventing identity fraud?
Professor Anderson: The words "identity fraud" are not used on the continent. The people who try and market it express frustration from time to time.

Q218 Mr Benyon: Because of what you were talking about earlier, about it being a cop out for the banks and a devious method of governments imposing—?
Professor Anderson: Because of it being a liability management technology and things have panned out differently in other European countries. Also, a significant difference between the UK and the continent is that there is much more vigorous enforcement of data protection law over there and this makes a real difference. The regulatory regime in Germany, for example, is quite different from the regime in Britain and also the bank regulation regime is different so the pressures and the drivers are different.
Mr Bramhall: I would agree with the point about the motivation in Europe being around stronger data protection. Absolutely. Interestingly in the Far East the member countries of APEC are starting to realise that perhaps they have a privacy issue as well. Obviously the tiger economies are doing extremely well with rises in the size of consumer class and concern is starting to surface there about participation in the online economy. Because there is a much wider diversity of cultures, social norms, political systems and so on in APEC compared with the EU, they do not really have the ability to take the same approach to privacy from a philosophical sense. The European approach is clearly driven from Article 8 of the European Convention on Human Rights. There is no similar kind of instrument in APEC but they realise they need to do something. There is APEC activity going on to formulate guidelines which will be common across the APEC countries. That is still very much work in progress. It looks like it is going to be written around avoiding the notion of harm rather than things like rights to know or rights to be protected against others knowing and so on. There are definitely different

models. In terms of how the technology fits, hopefully the technology is neutral and can be applied in a number of different models.

Q219 Chairman: If we all learned to stop saying "identity fraud" and started talking about the crime of impersonation, what practical difference would it make?

Professor Anderson: It would make marketing certain agendas much more difficult. To look for practical solutions using available, reasonable regulatory instruments, one probably has to look at the industries in which particular behaviours have become embedded. For example, if one is looking at credit reference agencies, they are regulated better in the USA where, to give one example, you can opt out of having a credit reference given. You can go to Equifax in the States and say, "I forbid you to ever give a credit reference on me to anybody at all." If you are middle aged, you have your mortgage and you have enough credit cards, that is great. You do not need any further credit. You have the immediate benefit that you get an awful lot less junk mail. Nobody sends you offers for credit cards et cetera.

Q220 Chairman: I am as keen on ID cards as Mr Winnick is opposed to them. I am quite prepared to go round persuading people that they should have ID cards to protect themselves from impersonation rather than identity fraud. A lot seems to be hung on this issue of language but I cannot quite see that if we went back to the old language of talking about impersonation rather than identity fraud it would make a blind bit of difference to any of the issues that we are talking about today. It seems to me to be a semantic argument but you clearly think that somehow by talking about identity fraud either government policies would be different, or bank policies would be different or something. I do not really quite understand.

Professor Anderson: The fundamental issue is an issue of liability. If a bad person whom I have never met goes to a bank with whom I have never done business, how should that be able to ruin my life by causing the debt collectors to call on me and causing all sorts of other derogatory stuff to be propagated about me through the system? It is clearly bad that such things happen. How do you go about stopping it? I suggested in our written submission one practical way of stopping it, namely that the Information Commissioner should enforce the existing law against the credit reference agencies. In the absence of that, what other policy options are available? One can debate this at a number of level. At the legal level, one could talk about various possible private remedies but, at the political level, surely politicians should set the tone for the debate, shaping the debate and deciding what sort of language is used. My point is that the language about identity theft is not helpful from the point of view of consumer rights and security economics.

Q221 Mr Streeter: Focusing on regulation, we mentioned this point earlier about the importance of individual responsibility as consumers and education to make people aware of risks. In terms of protecting privacy, apart from individual responsibility, apart from technological advances in terms of security, can we focus for a few minutes on what could a government do to regulate this incredible market place to protect people's privacy more? If you were advising the UK government, each of the three of you, what is the one thing that they should do which they are not doing? What is the thing that the government should do in terms of regulation?

Professor Anderson: The one thing I would do had I the legislators' power for a day would be to change the UK rules on legal costs to the American rules. In America, constitutional matters, which in this context would mean section eight of the European Convention on Human Rights, can feasibly be enforced by individuals. A young law lecturer wishing to win his spurs and become a professor can go to the Supreme Court and litigate. He does not have to face the prospect of paying $10 million in costs to the government if he loses. That right of private action is not present in Britain because of our rules on costs. That means that there is an assumption that all these actions have to be state actions. As a practical matter, we have an embedded Information Commissioner's Office which was designed back in 1981 to be ineffective. David Waddington, the then Home Secretary, at the time was quite open about the fact that it was a minimal implementation to keep us legal with Europe. Although the ICO has expanded his gamut somewhat since then, it still remains a very weak body. Are we to wait 50 years for successive ICOs to build up their clout within Whitehall so we can enforce constitutional law? If you want constitutional enforcement to be available to citizens, you have to make private action available as well as public action. That is why I would say let us move to the rules that they have in America or, if that is unacceptable to judges, let us move at least to the rules that they have in Germany where there is very much stricter limitation on taxation on the scale of the costs you have to pay if you lose.

Q222 Mr Streeter: That is a surprising answer but it is slightly outside the box of my question, is it not? It is a brilliant answer and, as a lawyer, I am all in favour of it but surely the government can do something top down as well at the same time as changing the rules on the costs of litigation?

Professor Anderson: The government could do something top down if, for example, the kind of law and practice that one sees in France and Germany on privacy were imposed on government departments, but again you come down to the question of the individual departments and their incentives and how power works in this town or indeed in any town. One suggestion that we made to the Information Commissioner's office was that he should see to it that the data protection officers in various government departments report to him rather than the departmental Parliament secretary, along the lines of CESG cryptosecurity officers reporting to Cheltenham rather than locally. That

way, the data protection officer would see his job as enforcing the rules within the department rather than seeing to it that the department has an easy ride with the Information Commissioner. These are all very difficult things to do because they are not the sort of things that you can do easily by means of a simple statute law. How you go about changing a culture of half a million people that has been 800 years in the building is hard.

Dr Phippen: The witness on my left might disagree with this but I think one of the big issues is tougher regulation of the IT suppliers and providers themselves. I spend quite a lot of time trouble shooting between small businesses and it seems to be web development companies in particular who will behave incredibly unethically in terms of what they are going to charge people for. It is a classic case. If you offer an IT supplier half a billion pounds, of course they are going to say, "Yes, we can do it." Why would they not? They will think about the technologies afterwards. At the moment you are looking at the IT "profession". You have a long way to come to achieve the levels of professionalism that exist in other professional practices such as law, accountancy and the medical profession. I think it is getting better. The fact is that the British Computer Society is talking with the government more now. There is a growing code of conduct there but it could possibly do more to make suppliers more responsible for what they are promising. I had a colleague who used to describe IT departments as having all of the power and none of the responsibility because they say, "You signed the spec. That is what you asked for." That kind of thing is changing a bit but it still has a long way to go if you are getting true professional liability within IT professionals.

Q223 Mr Streeter: It is all your fault. Do you want to apologise?

Mr Bramhall: I am just thinking about the phrase I used earlier about not tarring everybody with the same brush and how perhaps it might apply. There are two points, one regarding professionalism which I know is not your question but, yes, increased professionalism has to be good. There is in the information security space a new Institute of Information Security Professionals, for example, which is just coming into being and will hopefully have an impact on—I hesitate to use the word "standards" because I do not mean it in the regulatory sense—raising standards of quality in that space. In terms of the specific question you asked about regulation, I must admit I am coming at it as a technology research manager and I do not really feel confident to comment on that side of it, certainly not to the level of detail that Professor Anderson has done. Similarly, we have not conducted any research into the effectiveness of the ICO's power and therefore we should remain silent on that point as well. In general HP does support any actions which the Information Commissioner takes which will increase the general level of confidence that people have about participating online.

Q224 Mr Streeter: I cannot get my mind around the difference between UK regulation and global regulation. So much of this obviously is accessible globally through the worldwide web. Professor Anderson, you have mentioned other European countries which make a better fist of regulation than we do. To what extent is this industry capable of regulation nationally as opposed to internationally? Is there some more regulatory action that should be taken internationally and globally?

Professor Anderson: There are two different issues there. You get better regulation of privacy in France and Germany because you have different constitutional settlements that essentially predate automation, or largely so, or at least go back to the sixties or seventies. In Germany you have privacy written into the Constitution for reasons that are not particularly surprising. In France more recently there has been a dispensation that CNIL, which is their equivalent of the Information Commissioner's Office, is consulted by government departments while they are proposing new system developments and has a veto or something that in practice amounts to a near veto. The second issue which Andy raised is why is the government so awful at developing computer systems. It is generally reckoned that 30% of large IT systems in the private sector fail and 70% of large IT systems in the public sector fail. That was an admission by the Department of Work and Pensions CIO at a conference last month. We have all known this for a while. Why does it happen? FIPR has talked extensively on the subject. My FIPR colleague, Jim Norton, put together a programme and tried to get our ideas across to permanent secretaries. The gist of the FIPR take on this is that there should never be another government IT project; there should simply be business change projects. Ministers should cease seeing the purchase of a large IT system as a displacement activity, as something that will kick a difficult problem into touch, for the next government to worry about. Instead we should have a discipline that if somebody wishes to change the way their department does business, they should specify that and engineer it properly. If IT is part of the solution, then fine. We have been unable so far to sell this idea to Whitehall. I am sure its time will come sooner or later. From the point of view of privacy, some people might take the view that perhaps it is a good thing that 70% of large government IT projects fail.

Q225 Ms Buck: We have covered quite a lot of the questions that I was asked because we have been dipping in and out on a lot of questions about trust, risk assessment and things of that kind. Can I go back to something Professor Anderson said earlier about what it might take to change public consciousness? You used that very vivid language of a few dramatic stories on the front pages of the red-tops. You were teasing us a little bit with some thoughts about where that might come from and what it might mean. Can I ask about the research on trust and break it down into categories? What we have tended to do in the last couple of hours is weave

in and out of different groups of people and what they mean by trust. There are very different issues—and perhaps you will give us an idea about this kind of risk analysis in greater detail—between children and what children understand and what parents understand about children and risk; about young people and what young people think about risk and about the long term implications of their behaviour, knowing as we do that young people tend not to think long term; and also about adults and their levels of risk and what it might take, perhaps in those different categories to be the shock that requires people as individuals and people in relation to government and the private sector to get some changes.

Professor Anderson: The relevant research here is perhaps that of George Loewenstein at Carnegie Mellon University, who is a behavioural scientist and looks for example at the extent to which people overestimate the happiness that they would get from a good event in their lives or underestimate the sadness that would result from a bad event. He looks for example at how happy people are who are paraplegics or who have had an arm or a leg amputated after cancer, and finds that, although most people think that having an arm cut off would be the end of the world, in practice within two or three months people adjust just fine. They report that they are just as happy as they were before. The lesson that he draws from this is that the public's sensitivity to risk basically relates not to the absolute level of risk but to the change in the perceived level of risk. In other words, if a level of risk or threat increases very, very slowly, you will get occasional grumbles from the public, but you will not get a great outburst. He refers to this as the 'boiled frog syndrome' after this apochryphal idea that if you put a frog in cold water and boil it it will not jump out. His concern about this is in the context of global warming, that if planetary temperature continues to rise by a per cent every few decades without a dramatic shock the public will never get sufficiently agitated to demand that politicians do something. It strikes me that exactly the same argument applies to trust and to privacy, in that if privacy is slowly eroded then people will get used to it. We might end up in a society that is rather different from our society today and some of us old fossils might, in our bath chairs in our eighties, be grumbling very noisily about what has happened to the world, but there will not be a great outburst. If you get a series of shocks all at once, then that may change and public concern may suddenly spike and create the window of opportunity for regulation. This of course can cut both ways. It may very well be that the large number of privacy-invasive systems that government has built or talked about building over the past two or three years will together give that spike. Maybe ID cards plus kids' databases plus NHS databases plus ANPR plus and so on finally will hit critical mass and the public will go ballistic. We do not know. This behavioural research would strongly suggest that that is what politicians should watch out for.

Dr Phippen: Our work with young people would suggest that they do not really take any risk analysis when going online. They just go online.

Q226 Ms Buck: We can all vouch for that, with kids.

Dr Phippen: With 100-odd kids we spoke to, we had probably three clear cases of stalking going on and not one of them reported it to the police or went any further than, "I just blocked them from my MSN". "Why did you not report it?" "I did not know how to." "Did you think there was anything dangerous there?" "No, I just thought it was some weird kid and ignored them." The work that CEOP are doing at the moment is making great strides forward in that they are getting into schools. One thing the kids are all saying is, "We do not really cover this in school." When you have a look at the IT and the computing curricula for both GCSE and A level it is not covered at all and they say, "We might touch on it in citizenship", but again it is not covered a great deal. We are hopefully going to be doing some work with CEOP in the near future, looking at kids' responses to that. That is something that definitely needs doing. You have essentially a captive audience with children. You can go into the schools and talk to them. Initially they might say that it is a load of nonsense or whatever but it gets through to them and they do think about it. With adults, it is more interesting in that they start off looking at how you can get people to trust systems. What we realised very quickly was that trust is not really an issue. The issue is convenience and restitution. What people will do is look at the service on offer and think: what is in it for me? What could go wrong? Has anyone else used the site before? If it is fairly positive, then they will probably go for it. When you talk to them about why they go online, they say something different. We spoke an awful lot to people about what makes them use a website and an awful lot of people said that you need human contact at the end of it. It is not just the website. When you say, "What is your most trusted brand on line?" Amazon continually came up as the most trusted brand. You never deal with a human on Amazon. "Yes, but I have a mate; something went wrong and they rectified it very quickly." That is the thing Amazon do very well. They do not say, "This will never go wrong" but when things do go wrong they rectify them. They do not try to hide from them.

Q227 Ms Buck: You make an important point in your report about restitution but how can we learn that lesson from Amazon and expect, either within the private sector or in terms of government's duty in relation to the private sector, to be able to apply that restitution?

Dr Phippen: I feel a little sorry for public sector IT in that you do not have the commercial incentive there that you generally have with the private sector. The first thing to look into is the convenience, which is why the closed systems like DVLA and school registrations work. It needs to be a case of: what is in it for me? What am I going to get out of that? It does not have to be financial; it could be time saving or saving them having to go to local authorities and deal with something like that. I think it is a little more difficult in the public sector because there are immediate convenience measures that you can take. I do not think security

is a massive issue in either the public or the private sector. I always think back to education but I think it is the major point. The big concern is people believe that, if they buy something on their credit card and something goes wrong, it is the credit card company's problem, not theirs. Obviously credit card companies are back pedalling from this a great deal at the moment. They do not realise the long term damage in terms of credit referencing and those sorts of issues where, even though they might have had it rectified and they got their £500 back, they might not have gone down the chain and it could ultimately end up with them having a poor credit rating as a result of something. They are not aware of these issues.

Q228 Ms Buck: None of this would lead you to conclude that there is a public readiness in any of those categories to invest time or money in a personal solution? I am not saying that one exists but, were there to be a technological fix on offer or some steps that they could take which would involve some effort and some expense to protect themselves against some of those risks, there is not the public awareness yet to support that?
Dr Phippen: I do not think so. Tom Illube was behind Egg and is now in charge of Garlik. He spoke to the parliamentary IT committee a while ago. He said that when he was at Egg they did a lot market research for their customers so security is important so they introduced another factor to their authentication process and people stopped using it because it was too inconvenient. They cannot remember all that. I mentioned multiple identities. Most people have multiple identities all with the same password because, no matter what security experts say, you cannot possibly remember 30 or 40 alpha numeric, random strings. I do not ever think there is going to be a silver bullet technology that sells all this because there should not be IT problems or technology problems. There should be process problems which perhaps IT will address. I think the public are aware of that as well. They do not go online because everyone is telling them to. They go on line because it is of benefit to them.

Q229 Ms Buck: To paraphrase, we should raise the school leaving age to 25 in order to be able to accommodate a massive public education programme on this.
Dr Phippen: The biggest problem is the people who have already left school, between the ages of 18 and 60. In those cases, the media have a very strong role to play because all these people tell me, "You should not go online because how do you know that? I read about it in the paper or I saw it on the television." The media obviously are going to be far happier reporting on identity theft or government IT projects going wrong than, "Here is another successful use of IT in society." That is not sexy. That is not interesting. The media have a great responsibility to play in education.

Q230 Ms Buck: Does that make you feel optimistic?
Dr Phippen: No.

Q231 Gwyn Prosser: I have gained the impression from all three witnesses to different degrees that the public are very relaxed about these issues, whether it is CCTV cameras or going online or sharing their personal details. It is mostly certain classes and the media that are making a noise about big brother. You have given us the warning that as these layers of potential intrusion build up we should take a wake up call because it might suddenly come back with a public reaction an a resistance from the public. Is it not a fact that using CCTV, which is perhaps separate from your line of expertise, when it was first introduced in this country, created concern but over the years, as it has increased in areas of surveillance and as these other layers have come on with regard to the internet et cetera, people have become more relaxed about it and in some cases, especially camera surveillance, are demanding of politicians to have more in their patch?
Professor Anderson: The most telling criticism of CCTV is that the money could be better spent on other things. When we did the Information Commissioner's report on the children's databases, we looked at various crime reduction initiatives with a multidisciplinary team. In 1997 the government started off with some very admirable and well-researched initiatives including Communities that Care, an initiative whereby people would be got together in tough neighbourhoods—stakeholders, policemen, ministers, councillors, whatever—and would be consulted about what the best crime reduction measures would be for that neighbourhood. The Home Office no doubt would have a budget to spend on these. Similar programmes have been effective in the USA. However, what appears to have happened—there is a reference in our written submission—is that this was subjected to lobbying by the CCTV industry and instead one had programmes to the effect that, "We will give you money for an initiative provided it involves CCTV." This appears to have been one of the reasons why the 'Communities that Care' initiative was not as successful as might reasonably have been expected. Yes, there may be some placebo effect from having large numbers of closed circuit television cameras around, but the analysis of the crime statistics which we cite tends to show that although they are good at reducing crime in car parks they are not so good at reducing crime in town centres and there is a very serious question about whether far too much money has been spent on these and not enough money on other crime reduction initiatives.

Q232 Gwyn Prosser: To what extent do you think the increase in the sophistication of technology to enable the state and private enterprises to scrutinise people's personal information and have access to it will, on that side of the equation, compete with the increasing potential for individuals and companies to protect themselves from that surveillance? Where are we at the moment and how do you see that tension developing?

Professor Anderson: One of the big tensions that we see developing is that of equality of arms and the balance between private and public action. At present it is very easy for the police to get hold of CCTV data or ANPR data to prove that you did something bad, but it is a lot more difficult for you to get hold of it to prove that you did not, to establish an alibi. When we move into the realm of civil cases, for example disputes between customers and banks, the same issues arise. The banks can get CCTV data but you cannot. There are also issues about, for example, how you go about tracking people. The Information Commissioner a couple of sessions ago remarked that there had been a website which enabled people to track individuals in the UK from electoral roll data. This provoked an outcry from people who had perfectly good reasons not to want to be tracked. It was accordingly shut down by the Commissioner. Yet again, many new pieces of surveillance have to do with people trying to track other people. What sort of mechanisms should be available for someone who has a *bona fide* reason to want to track down another person? We suggested in our written submission that if there was some means whereby, for example, a wife who was seeking alimony from an absconded husband, and had got fed up with the delays involved in the government mechanisms for doing that, should be able to go to a court and get an appropriate order to get information from relevant databases to find where hubby is living and where he is working so that she can go to the court and get an attachment order against his wages. Again, these all have to do with the fact that surveillance centralises power. Whether it centralises power in the hands of the state or in the hands of large corporations, it raises all sorts of issues: equality of arms, public versus private action, but I think that successive governments over the next few years are going to have no choice but to think about it.

Mr Bramhall: Right at the beginning of your previous question, I think you said that people are very relaxed about participation and so on. The TrustGuide work showed that that was not the case, and that there was a general unease. It was not a specific unease, but there was a general unease and a wish to move forward.

Q233 Gwyn Prosser: But not sufficient to discourage them from using that access?

Mr Bramhall: No. And again different people took different views on that. TrustGuide was not meant to be a large, statistical sample. It was more qualitative but within the collection of people who participated there were some who felt quite comfortable, some who did not and some who never have but probably would not because of something they have read about. I do not think we can say that people are very relaxed. They are generally uneasy but, you are right. It does not inhibit them.

Q234 Gwyn Prosser: Professor Anderson, you give us the prediction or caution that we will need a number of headline stories in the tabloids about the hard cases before we perhaps wake up to some of the concerns. If you were to look 20 years hence and take into account that these various changes in public perception of policy can take place, would you expect that the private sector and government would have overall more knowledge about us as individuals or less?

Professor Anderson: They will have more knowledge but it will be much better regulated. We have seen the beginning of the push back, for example, on Google, with Google now agreeing to de-identify personal data after two years. This is remarkably quick. The issue was raised first at a conference in France in February[6] and now it is already actioned. It is high on the European agenda, so these things move up the political agenda as more people become aware of them. The hearings that we are having are, I believe, driven by the fact that there is general raising of public awareness, bringing surveillance onto the agenda. One cannot stop the collection and processing of data becoming cheaper because technology advances, but as it affects more people and perhaps also more interests within society, more organised interest, you are going to get a push back because, after all, what tends to stop one large, powerful lobbying force is not people speaking fine words and arguing from principle but the opposition of other large, powerful lobbying forces. Just as the whole intellectual property debate came into balance when the music industry started being faced down by the supermarkets et cetera, so I would expect that in due course, in the private sector, the action of the Googles, the Microsofts, the Yahoos and other big players will evoke enough lobbying response from those businesses that are losing out.

Q235 Gwyn Prosser: More information and better regulated?

Professor Anderson: More information and better regulated.

Dr Phippen: I would certainly agree more information and hopefully better regulated in the next 20 odd years.

Mr Bramhall: I agree that more information will be known. I agree also that it will be better governed or the governance will be better. Some of that might come from better regulation for the reasons mentioned. I suspect that will be rather patchy. I think it would be true in the UK and Europe. I am not sure we can take that as a global statement. Where regulation is not the motivation for the improvement, also there will be some motivation from individual private sector enterprises wishing to differentiate themselves again by being seen to do a good job and being more trustworthy. That is less determined by whether they're UK, Europe or the rest of the world.

Chairman: Thank you very much indeed. It has been a very useful session.

[6] *Note by witness:* Sorry, January—Economics of the Software Industries, Toulouse, Jan 18–19; the relevant discussion was on Jan 19th.

Tuesday 26 June 2007

Mr John Denham, in the Chair

Mr Richard Benyon	Margaret Moran
Ms Karen Buck	Gwyn Prosser
Mrs Ann Cryer	Martin Salter
Mrs Janet Dean	Mr Gary Streeter
Patrick Mercer	Mr David Winnick

Witnesses: **Professor Carol Dezateux**, Institute of Child Health, University College London, **Dr Ian Forbes**, Royal Academy of Engineering, and **Professor Simon Wessely**, Academy of Medical Sciences, gave evidence.

Q236 Chairman: Thank you very much for coming to give evidence to us this morning. As you will know, this is one of a number of hearings that we have been holding under the broad heading of "A Surveillance Society?" taking our cue from a report from the Information Commissioner last year. We are very grateful to you for coming to give evidence and to share your particular expertise with the committee. For the record, would each of you introduce yourselves?

Professor Dezateux: I am Carol Dezateux. I am a professor of paediatric epidemiology at the Institute of Child Health, University College London, and I am also an honorary consultant paediatrician at Great Ormond Street Hospital for Sick Children.

Professor Wessely: I am Simon Wessely. I am Professor of Psychological Medicine at the Institute of Psychiatry at King's College London, and I am here on behalf of the Academy of Medical Sciences.

Dr Forbes: I am Ian Forbes. I am a social science consultant and an Associate of the Institute for Science in Society at the University of Nottingham. I am also here partly representing the Royal Academy of Engineering.

Q237 Chairman: Can I start with a question to Professor Dezateux and Professor Wessely. One of the things that you argue very strongly about on the accumulation of databases is that they have been of very public benefit and there have been gains to public health from the use of personal data for medical research. Could you indicate very briefly again what those benefits have been but also what you think the benefits might be in the future, looking at the databases and the science?

Professor Dezateux: Thank you for this opportunity to talk to you about the benefits of using patient data, which is sometimes called secondary research because it is using information about patients rather than necessarily contacting them. Really, without patient data, we would not be able to obtain the evidence on which improvements in health care have been based over some decades now. There are five groups of research that benefit from using patient data. Firstly, by using such data, we are able to identify causes of disease reliably. That is very important often for public health questions but also in terms of allowing us to move forward in ways to finding treatments. Secondly, it allows us to identify effective treatment precisely, quickly and in the longer term, and also to look at the potential adverse effects of treatments, which are often much harder to study. Thirdly, it is absolutely essential to have access to this kind of data to provide any public health monitoring in terms of control of infections and epidemics and pandemics, and also for us to be able to understand the effectiveness of any interventions, either at a health service or at other level, that are designed to control and constrain any epidemics. This leads on to the fourth point, which is really about patient and public safety. I do not think we can over-emphasise to you the value of this infrastructure in terms of being able to answer quickly, reliably and precisely in response to concerns about safety of medicines, safety of environmental issues or safety of vaccines. We can give you lots of examples of this. It is always the thing that you have not thought of that comes up and knocks you on the shoulder. Unless you have an infrastructure that allows you to do this, you are very disabled as a society in responding competently to these concerns. Finally, without the ability to look at patient data, we cannot evaluate how well our health services are doing and how well they are doing relative to one another. That needs high quality data that is complete and that that is given priority in the health service. What I would want to say really is that although these are called secondary uses, these are addressing primary functions of a health system where to protect and promote the health of our population, we want reliable information. In fact, we would not want to be looked after in a health service that did not provide an opportunity to learn from the data that we have collected and constantly improve health care.

Q238 Chairman: You will have seen the signs in the House of Commons on the way in that it is to be smoke free from 1 July. Is it fair to say that probably that sort of public health change would not have come about without the sort of analysis of patient data that you are talking about?

Professor Dezateux: Yes, that is an absolutely wonderful example. The original observation by Sir Richard Doll linking smoking to lung cancer relied exactly on patient data. As we have gone through the whole tobacco control process, it has been informed at every stage by this kind of data, and now we are looking to using this kind of data to see whether we are getting the correct response and results to this kind of intervention, and whether there are any sectors of society that are being excluded or who are

continuing, for example children, to be exposed and where perhaps we need different measures. It is important to think about these things in a dynamic way, and smoking is a very good example.

Q239 Chairman: Professor Wessely, in the Academy of Medical Science report, a reference was made to "inappropriate constraints on the use of personal health data". Given all of the positive things that Professor Dezateux has told us about the use of this information and data, what do you regard as the inappropriate constraints?

Professor Wessely: What we meant by that is that there is a framework that allows this kind of research to go ahead, a very well worked out, ethical, legal and governance framework, but there are times when many people are intimidated by things like the Data Protection Act or the common law, usually we found through ignorance of the legislation, and do not allow research to go ahead. Our studies of cancer in Gulf War veterans, for example, had great difficulties in being done because people felt they could not release data from cancer registries. It took about three years to overcome that. That is our general point. We have a well-established, very careful—possibly over-cautious—governance framework to allow this, but we found innumerable examples of good research that was being impeded by people's ignorance of things like data protection, although to be fair, if you read the Data Protection Act, which I had to do, that way madness lies. It is not written to make it easy, but in fact it is a perfectly sensible piece of legislation that, if you work it through, allows proportionate invasion of privacy for public health research, but you would not know it if you read it.

Q240 Chairman: The phrase "surveillance society" conjures up a rather Big Brother image, which is why we put a question mark at the end of the title to our inquiry because we want to take a balanced view. Could I ask the two professors: do you regard the sort of work that you are advocating as part of a surveillance society? Do you feel happy with that tag?

Professor Wessely: It depends what you mean. At the moment, we are carrying out health surveillance into the health of the Armed Forces. We are looking at the rates of post-traumatic stress disorder, the rates of cancer and the rates of all sorts of other adverse outcomes. That is surveillance because it is based on medical records, cohort studies and research, but most people in that context would think that is a good thing. Certainly the members of the Armed Forces think that is a good thing and they are appreciative that this has finally been done. It all depends on the context. Health surveillance is actually a good phrase and we would agree with looking at the effects of MMR vaccine or surveying the effects of the Vioxx drug, and we are not talking about hidden cameras in supermarkets.

Q241 Chairman: Dr Forbes, we are going to come to your evidence a little later on but do you have any comments on that opening exchange?

Dr Forbes: I am delighted to hear this positive use of the term "surveillance" because I do not believe there is enough awareness of the way that society is constantly 'surveilled' by a range of systems, mostly governance systems, to increase our knowledge of ourselves, to provide information which leads to better knowledge and better insights to wisdom so that we can make really quite crucial and large social decisions based on the information that we provide by just living or dying. This is a good example of how data can be collected, how it is managed. If you think about the safeguards that attend to medical records, they are extremely sophisticated. There is a worldwide practice about how to do this and how to manage anonymity and privacy, and yet it is used to be extremely constructive and to provide us with the sort of data that we need and I think that is missing in other areas of society.

Q242 Ms Buck: Can I pursue the line about data? Are you confident that the medical research that you undertaking requires analysis of databases rather than research that would be done by using volunteers, for example?

Professor Dezateux: I think that we need very large-scale evidence for a lot of the questions that are facing us now. At one level, therefore, just approaching individuals is simply not feasible. The reason we need large-scale evidence is that we are dealing often with things that are quite uncommon but about which it is important that we have reliable answers. These could range perhaps from the association of birth defects with certain drugs that are given to women in pregnancy to the relationship to birth defects with power lines, mobile phones or any of those sorts of things. Birth defects are a good example because they are uncommon and you need data from the whole country. It is clearly also obviously data that you are not going to be able to go back to necessarily and get. The importance, from an epidemiological point of view, is that our science is served by giving answers that are not biased and that are not misleading in any way, that are precise and timely and where we can also compare groups of people who are not exposed to the thing we have been asked to look at. All those things really support the need to have large-scale evidence. I can give you any number of examples of issues that in fact parliamentary committees have sat on, such as assisted reproduction and so on, where we really are tied by not knowing answers to the sorts of questions to which we should have answers because we have not been able to get access to large-scale evidence. The other point to make about this is that the kind of research that epidemiologists do is concerned to get information right at the individual level, but we are not concerned to identify or know who that individual is; we are interested in that individual because they are part of a group of individuals and we are interested in things at the group level. From that point of view, large-scale evidence based on patient data is one of the best ways that you can look at highly sensitive information because it is possible to have very good safeguards and security and you do not stand the

risk when writing to somebody of exposing to somebody in their house that you know something about them inadvertently, as you might do when you have to approach at an individual level.

Q243 Ms Buck: Professor Wessely, you said earlier that there was a robust system of governance for undertaking this kind of research but yet, at the time, problems arise and research does not necessarily go ahead or there is controversy over progress because people do not understand that. If it is as good as you say it is, why is it that people then doubt it? To what extent is that to do with concern over issues around individual consent and the anonymisation of data?
Professor Wessely: First, most research goes ahead with consent, and that is the default position and you start from that. Obviously, for any interventional research—if you are going to give people a drug, a new test or some procedure—you have consent; if you do not, you are committing assault. We put that to one side. Research based on data usually goes with consent, where that is practical and possible. That is normally what we do, so our studies—and I have just mentioned the surveillance of the Armed Forces—are based on consent, but there are times when that is not possible. If I gave you a practical example, then it would make sense to you. We wanted to look at the association between depleted uranium and cancer, and this may appeal to Patrick. Therefore, we have 100,000 people who have been potentially exposed in the Armed Forces to depleted uranium and many of them wanted to know whether or not this had led to cancer. To do that study, it is not possible to approach 100,000 soldiers, most of whom have left the Armed Forces. Nobody knows where they live; they do not use landlines because they tend to use mobile phones now; they are almost untraceable and it would cost millions of pounds and you would miss the very ones that you want to find. First of all, you need ethics approval. In fact you need two sets of ethics approval. You cannot do any research without ethics approval. You need to use a system called the Caldicott Guardian. This is for the people who hold that data, namely the MoD or the cancer registries, to permit you to see that data. It is a very complicated procedure which you have to go through. They hold the data and they have to decide if this is a reasonable thing to do. You need permission from something called PIAG, which is a Department of Health committee, that oversees this system and adds an additional layer of governance. You have to comply with the law. You have to show that there is not any other way of doing it. You have to show that no one is going to be upset or distressed by this. You have to show that no one is going to get any individual detriment from the loss of this data. You have to show that you owe a duty of confidentiality and that there are sanctions in place if you break that. That has never happened. There have been no instances of medical researchers leaking confidential data. That is not to say it will not happen but it has not happened yet. You have to belong to an organisation that says that if you do that, you are fired. There is a whole complicated system of checks and balances in place before finally you are allowed to link members of the Armed Forces and their rates of cancer. In fact, the answer was that there is not an association. There is no other way of doing that kind of research.

Q244 Ms Buck: What I do not understand then is with so many locks on protection of the data, why it is that anybody anywhere should ever raise concerns about proceeding with particular research?
Professor Wessely: There is no question that many people do not know this system. I think that is quite clear from the Academy's report. A lot of people, and within the profession itself, to be frank, are ignorant of this framework, partly because it is very complicated. I think also there have been instances of misconduct in research or misconduct in the health services that tar every one with the Alder Hey brush, if you would, which are not relevant at all to what we are talking about but have created a climate of suspicion. Finally, having said that, when you look at what the patient charities in heart disease, Alzheimer's and Parkinson's want, unquestionably they want this kind of research to go ahead.

Q245 Ms Buck: I am sure we will return to many of these points, but as my last question: the Academy's report criticised what it calls the over-rigid application of the principle of "consent or anonymise". What you have described to me is a system that has so many locks in it that it does not seem to justify any deviation from this principle. Why is it that you would be looking for, and what benefit would there be from, a reduction in protection through consent or anonymisation?
Professor Wessely: First, "consent or anonymise" was the principle, for example behind PIAG, the idea that eventually you would either have consent or anonymisation, but that is clearly wrong. The whole point is that there are many times in research where you cannot proceed with that. Our study of Gulf veterans could not proceed on that basis because if the data had been anonymised, we would not know who they were and we would not be able to link them up with their cancer rates. So it was a flawed principle. Therefore, there are occasions when you have to be able to proceed without consent and without anonymisation. I have explained that that is unusual but it does happen. What the Academy is saying is that, first, people are not necessarily aware that these examples exist; they are not necessarily aware of the governance framework; or most of them misinterpret it to say it is "consent or anonymise", which is absolutely not the legal framework we have. It is not the framework behind Connecting for Health. It is not the framework envisaged in the Data Protection Act or the law of confidentiality.
Professor Dezateux: The first thing to say is that one person's anonymised data and identifier is another person's research data, and so it is very difficult to look at the same piece of information and make a clear decision one way or another. Given that is the case, we have to use common sense and we have to ask what are the safeguards when we use this information to avoid disclosing the identity of a

person while still being able to answer the question that we think is important. One of the interesting issues is that it all pins on individual consent. We need to move away from that paradigm a bit and ask what processes there are for community assent. It is ridiculous that we cannot answer some of these questions because that is the side on which we often find ourselves. The other thing that I hope we will have a chance to discuss is the greater clarity of the processes because with a lot of the public misunderstandings and understandings, we could do with a better communication strategy. That applies to people operating and interpreting these things at a health service level. The sort of people we need to negotiate with about access to data are sometimes also confused, and that is not surprising. At a scientific level, there are many reasons why we need to know things about people. Again, we are not interested in who that individual is, where they live, but we need to know certain things about them in order to practise better science and to produce a more reliable answer. We need to know that we are not double-counting. You need a couple of common identifiers to make sure that you only count an individual once in your data. We need to be able to follow people up in the very long term. That is becoming increasingly important. We are interested in diseases and treatments for things like cancers which might take a long time to develop, and we need that kind of information to be able to trace people. If the data are anonymised at the beginning, we cannot do that; we cannot get back to them. We need to make sure that the data we produced from our health services is respected and that it is of high quality, and that when it says this person has a condition, they really do have that condition. In fact, we know that sometimes there are mistakes in the basic health service data. Research can help the health service improve the quality of its data by being able to what we call pseudonomise, to have ways of getting back to say, "Was this really what we thought it was? Do these people have this condition or have they had this operation?" Then, as I mentioned right at the beginning, without data that is potentially disclosive, such as postcodes and so on, we are not going to be able to say whether cancers are related to power lines or living near nuclear power stations or any of those kinds of questions that I believe you would have an interest in getting the answers to as well.

Q246 Gary Streeter: You have talked about checks and balances but does it not worry you at all that some of the information that you are overseeing the gathering of is being used and will increasingly be used to produce some of the genetic modification type science of the future? Does that ever cause you sleepless nights?

Professor Dezateux: There are serious issues that society needs to debate about the use and application of genetic advances. I do not think that those issues will be resolved by saying, "We are just not going to use the data at all". Indeed, I think that where it is helpful is for us for example to be able to link somebody's biological data to their health and their future health status, you can begin to put boundaries round your uncertainty about what the meaning of this genetic change is—whether it is helpful to know about it, whether it has any implications at all—and then inform the health services as to how appropriately we should be using that test within the health service and, bearing in mind that there is a very big private market in genetic testing, to inform the public really about whether it is wise or advisable to get tests that might identify a prediction for disease or not.

Professor Wessely: If you look at the UK Biobank, which is an example of research in genetics, 60,000 people were approached and asked to take part and only 50 people objected and of those 50, 30 then consented to take part in the study. So, within the framework of research, people are confident in the use of genetic information to study disease and are willing to participate.

Q247 Martin Salter: Professor Wessely and Professor Dezateux, obviously you would be disappointed if we had not put you under intense surveillance before you came before us. Because we have a phalanx of staff, we have dug up your interchange with Dr Richard Taylor at the Health Committee on 7 June, which is very informative. My question relates to that. Just to paraphrase, Richard was questioning your contention that perhaps medical researchers should be given more access to patient records than even the police. We want to give you an opportunity to expand on that. It appears from the exchange that you were implying that the public would trust you perhaps more than they would trust the police. You may be right.

Professor Wessely: I am not implying that. I think that is a statement of fact, is it not?

Q248 Martin Salter: And your evidence is?

Professor Wessely: I think I mention it. We did a study around the polonium incident about who do you trust to manage this incident, and doctors and scientists rated much higher than the Home Office and the police force. More seriously, there is a misapprehension there. If you want to look at personal data, the Data Protection Act actually says quite specifically that you cannot do that to make any decision about an individual without their consent. The police would only want to access data to make a decision about an individual: is he a crook, or whatever. That is specifically illegal. You cannot do that and we cannot do that, but that is not why we want to look at data. We are interested in not one child with autism or one child who has had a vaccine. We are interested in all children with autism and all children who have had the MMR. In that sense, it is not a personal piece of data about that individual; it is about all the children who came under that category. That is the framework for which we use that data, and that is the framework that is already permitted by the law for the public good. That is the specific framework that denies the police access to the same data for making individual decisions. As a normal citizen, I can tell the difference between wanting to find out if living near a power station

causes leukaemia and wanting to find out if I have been naughty with my taxes or whatever it is. These are chalk and cheese and I think most people accept and can understand that.

Professor Dezateux: The answer is that both the police and biomedical researchers are subject to constraints, and I do not think we have unconstrained access to data. Simon has indicated quite how many approvals and permissions we have to have. The issue of whether we should be constrained in the same way as the police depends on why you are constraining the police and why you would constrain medical researchers. I suppose the thing that unites the police and biomedical researchers is that we are both interested in the elimination of doubt and the reduction of uncertainty but for our purposes, we need to have large-scale unbiased evidence to reduce uncertainty and make sure we have the right answer. The public's concern about the police of course is that they will get the wrong answer and somebody will go down who is innocent. In our instance, getting the wrong answer has public implications that it is really important to avoid. We do need that access but I think we should make the point here that we are not asking for unconstrained access, and we very much support the checks and balances that are there, but they need to be looked at in a flexible way. Also, I hope we will be able to come to discussions about how they can be improved.

Professor Wessely: You have already foreseen this in the legislation by saying that personal information cannot be used to that individual's detriment. If I was to do that—I cannot think how I would or why I would—I would be breaking the law and committing an offence and I am going to be in deep trouble. So there already is a framework to prevent the Orwellian implications, as it were.

Professor Dezateux: May I add that I think it is important that we are accountable. I consider myself a public servant in my research, as a lot of epidemiologists do. We are quite happy to be accountable for the work that we do and our approaches. Indeed, we are audited and have had our systems looked at in relation to the Data Protection Act and so on on quite a regular basis within our university.

Q249 Martin Salter: Thank you for your very full answers. How confident are you that medical researchers, having navigated the various checks and balances that you have in place, then are able to access for perfectly legitimate reasons personal patient information? How confident are you that that remains secure and could not be leaked to people who should not receive it?

Professor Wessely: There are two answers. First, when we took evidence for the report, the Information Commissioner confirmed that they had no reports to them of what you are describing happening. They had had reports of receptionists seeing things that they should not and all sorts of things within medicine of data violations but not involving medical research. I am not saying that will not ever happen but so far it has not. The second thing is that if we were to do that, and particularly in the new electronic health systems, you would leave a massive electronic fingerprint all over the place. It is quite straightforward. In my university, and I think in all universities, that is the end of your job, and it is also the end of your career because you would be up before the GMC. Even if you were to do that, you would leave a trace and that is it.

Professor Dezateux: When I started in research and I went into a primary care record, the Lloyd George record, I could read everything about that patient just by being handed the envelope, but now with technological developments, there is access control and audit trails. I think the chances of leaving a set of notes out on the table that somebody else can read are very much less. The computing infrastructure is much stronger.

Q250 Mrs Dean: Moving on to the NHS database, what opportunities will it open up in terms of medical research and epidemiology and what safeguards are being built in to protect unauthorised access to patients' records? Are those satisfactory?

Professor Dezateux: From what we have said before, it is clear that electronic patient records will provide a huge advance because they will allow us very effective access to the large-scale data that we need. I will not rehearse the issues about that. One of the things it allows us to do is to be inclusive in our research so that we do not leave certain sections of the population out. It can help us get swift answers. It helps us look at areas of medicine that we are often criticised for not spending enough time on in our research: rare disorders, under-served populations. It helps us look at demographic change in a dynamic way because we are a very changing population in the UK. One of the areas that we are interested in is that it allows us to link inter-generationally, so that a lot of the issues that we are concerned about are what happens to mothers/parents and their children and subsequent generations? You can be very powerful in answering those sorts of questions by using electronic records that can be linked by a single identifier. They are cost-effective. I think that we need to understand that after the Cooksey Report, there is a real recognition that unless we make the most of these electronic health records, we will not be able to maintain globally our competitiveness in terms of our science, and that will have economic implications for society. That is not what I come to work day to day to do but it is a very important issue, and it is an important issue for trials and providing an infrastructure for trials, just as much as it is an important infrastructure for understanding the safety of medicines. There will be investments in research that we will be able to attract if we are able to get this right and use the electronic health records effectively. The safeguards that are in place that we have described already are quite sophisticated for the kind of research that we do, and they would be appropriate for this kind of research with the electronic health records. There are plenty of examples in Scotland, in parts of England already, the Nordic countries, Australia, the US and Canada where there are systems in place that allow the data

to be kept in its own home, as it were, but for the linkage to be done by somebody who does not need to look at the data, so that the researcher at the end of the day just gets the information that they want and need on a need-to-know basis. I think those kinds of safeguards are very important.

Q251 Mrs Dean: Do you have anything to add to that?
Professor Wessely: I do not really. On the technical side, I would rather hand over to our engineer.
Dr Forbes: I am not an engineer but engineers become very nervous about single source databases, which have to be used by a large number of people and have to be designed for ease of input on a regular basis, and so there is a large number of users. The compromises that need to be made in engineering terms inevitably compromise the security of any single database. They are concerned about that and they say it is better to build in rather than build on. They say, "Let us think about how this system could fail and will fail either by misuse or by abuse or accident, all the ranges of human and technical possibilities". That needs to be thought about in advance. This has nothing to do with the way the research is conducted or the way that the protocols for research are developed. I am very happy with that. I am sure they are going to work very well. It is just that the matter of a huge amount of data being input by a wide range of users means that it is a single system; it has greater vulnerability and that needs to be acknowledged. It is a dilemma. You want the single database for all the social benefits that become possible by having the single database but that has to be weighed against the dangers. It is all about balancing those things. The engineers would say you should think about this in advance, design up-front, do lots of upstream thinking about how any human system is going to fail at some point in some ways, and work out what you are going to do about it when it does fail. I do not think you can get any further than that. You cannot produce a completely fool-proof system, so let us design it to assume that it will fail in some ways.

Q252 Mrs Dean: When it is up and running, how can patients be reassured that their own medical details are kept confidential?
Professor Wessely: First, if you read, for example, the Care Record Guarantee, which I think is a very sensible and remarkably plainly written document, it talks about the various checks and balances on confidentiality. Beyond that, there is also the moral and ethical framework—and I am talking specifically about medical research now because that is what I am interested in and patient care in particular—in which we work, and I do not think that climate has changed. I do not think doctors have become any less concerned with confidentiality, or the GMC has become less concerned with the advent of electronic patient records. It is presenting new systems but the ethical framework for the conduct of those systems is just the same. Personally, if I had gone to my wife's surgery in Kennington a few years ago to collect her, I could see on the desk the notes of everyone she had seen that day. They were in a big pile. Now I cannot do that; I cannot see them. We sometimes have a view of a rosy-tinted past in which doctors clutched case notes to their bosom and never let them out of their sight 24 hours a day. That is just not true. I personally feel more confident in the security of electronic matters and not least because again it is really important that if I mis-use them, the constraints on the system and the recriminations are so vast that that is a greater deterrent. In the past, I could wander into medical records and, quite frankly, if I wore a white coat, I could take out medical records; nobody would challenge me. You are right, there will be mistakes. Of course there will be errors but there is a system for correcting them and there is also a system for governance to make sure that if those are done maliciously, there will be severe penalties.

Q253 Mr Benyon: Before I turn to Dr Forbes, a doctor in a surgery in my constituency received a fax the other day from a hospital up north about a patient on their register who had self-harmed. This was just attached to his medical notes. The next time he came in, the doctor questioned him about it, and it was perfectly obvious that they had got the wrong person; he had the same surname and the same date of birth but he was a different person. Should we be concerned that information is floating around the country when mistakes are made of that nature that can have a huge impact on that person's life and job prospects if it became public?
Professor Wessely: Of course you should be concerned about that but that has always been the case. It has been far worse in the past. Notes could just get lost and you would never see them for years.

Q254 Mr Benyon: I should clarify that nobody seemed to know who should correct this information, whether it was the hospital that had made the original error or whether it was the GP surgery. There seemed to be no understanding about who owns that fault.
Professor Wessely: That is a governance issue. I am not *au fait* with how that works. I do know it is much easier to correct that kind of mistake now than it was in the past. It has always happened. Mistakes will be made and there will be a lot of John Smiths with a certain date of birth. Now, whoever it is, either the GP or the hospital, can alter the record whereas previously the notes will be there in perpetuity down in the bowels of the hospital and years later they will turn up and nobody would know they were mistaken, and, most importantly, the patient would not know that they were mistaken. I am not going into how this happens but now I know that patients will be able to check their records and they will be the first people who will say, "That is not me. You have made a mistake". Previously they would not know. They would have no idea what was lying on discharge summaries all round the country in the bottom of hospitals.

Professor Dezateux: The electronic health record will improve this because if we use a unique identifier, then one John Smith will not be mixed up with another. That is important. The second point is that you will not fax it so that this terribly disclosive information is left for anyone to read; you will send it by the existing system which works with Connecting for Health, which is encrypted emails and messaging services. Thirdly, to find that out, if you can access a single electronic health record, the information on the spine is visible to the person who cared for that patient and the GP who is looking after them, so there is instant communication, and the patient who should be able to access and look at their own record.

Q255 Mr Benyon: Dr Forbes, you have set out six clear principles to govern the use of surveillance data, the fourth of which says, "In general, public agencies should not be allowed access to private databases". Should the police and the security services be an exception to this and, if so, what conditions should be put on those exceptions?
Dr Forbes: I would say there should be no blanket exceptions. I would say there needs to be justification for access to a private database by a public agency because when I give information to a private agency, I am giving it to them; I am consenting for them to use it for their common purposes. There may well be cases where there needs to be or there is a very good case for access to a private database. The case needs to be made on a case-by-case basis. If, after a time, you think that there are so many of these cases, we need to have a rule or a rubric which would allow the police to invoke it, I do not see any problem with that in terms of a governance procedure. The NHS is a very good example that says, "This is what we want to use this data for and we therefore generate a series of mechanisms to make sure that it is not misused". They do not say, "Do what you like with the data". I do not think there is any case anywhere for saying, "There is data. Do what you like with it" just because you are the police or the security services.

Q256 Mr Benyon: Your fifth principle is: "Public record databases should be under the control of autonomous agencies, not government." What difference does it make?
Dr Forbes: There is a huge difference. The difference here is between the state and the government. I do not mind providing information to the state which uses that information for purposes which are about the collective good and the benefits will be indivisible; they may or not come to me. Governments have purposes for which I may or may not have consented. I may have voted for them, I may not. They may be doing something I like, or they may not. I think it is a good principle to say that the government has to justify the use of the data of its citizens. The government does not own me; it does not have any right over me. It is the other way round in fact. It is there because the people have put the government there. We consent to the state and we elect a government, which we can get rid of. I think that is an important principle. Public trust is very important. Trust in governments goes up and down, this way and that way, for good or bad reasons. If it also is going up and down in the same way on the state, I think that is potentially damaging for society and for politics in general because ultimately you want people to honour their commitment to the state and do what they like with the government.

Q257 Mr Benyon: Would you call the NHS an autonomous agent?
Dr Forbes: Yes, it is an autonomous agency. As far as I know, the government, cannot say, "Give me that" and just have it.

Q258 Mr Benyon: Your sixth principle relates to the penalties for misuse and you say that they should reflect the damage and distress that the system failure or crime causes. However, we all know that sentencing usually reflects not only the consequence of the offence but the culpability of the offender. Do you accept that?
Dr Forbes: Yes, I think that is a fair consideration.

Q259 Mr Benyon: Do you think, for example, that leniency should be shown in the case of a teenager who is particularly skilled at hacking and finds his way into personal data for kicks rather than for any malicious intent?
Dr Forbes: I do not know what leniency would mean. I think that you would treat a teenager as a teenager, first of all. I do not know about you but I am not lenient with bad behaviour.

Q260 Mr Benyon: In the United States, for example, they throw away the key. It is Alcatraz if you breach data protection. We have a slightly different attitude in some respects in this country.
Dr Forbes: That is about sentencing policy and how you treat adults and children. I do not think that is an issue about data, frankly. Teenage hackers will show you how vulnerable your systems are, so they are very useful in fact. To punish them for your own failures in your own systems I think is cruel. If I could just come back to your example of the fax, I think it is a terrific example where the specifications for a database, for example the NHS database, will have been, "We want a database that does this, this and this". Has anyone gone round and asked, "I want to know from all of you medical professionals what things have gone wrong that the system should look at and come up with some way of dealing with?" Instead of just a new specification, it is a problem specification. We know that this is going to happen; we know that this is typical; we know that that happens. Design it, please, not so that it is going to do all these lovely things but so that it will address some of these common problems with records that the medical service knows about. I think that is the way that you can build in protections.

Q261 Gary Streeter: Dr Forbes, you mention in your paper some concerns about the invasion of privacy caused by the four million CCTV cameras we now

have in this country, although they make our constituents feel safe and they want more of them, not fewer, I think. What are your concerns and can you give some concrete examples of this invasion of privacy?

Dr Forbes: I think having four million cameras is already an invasion of public privacy, which seems not to have been a consideration by members of the public. They have just given it away, in a way. There are examples of the way that cameras have been used to the detriment of particular individuals and groups of individuals, women for example. The next problem is going to be an extension of that, if there is no check or consideration about what the invasion that is taking place might turn into, because now coverage by cameras is mostly digitally stored, so it is there for ever. Like anything else, it is just data which can be mined, explored and new technologies and new software can look at that data again and again and pull more things out of it. Effectively, your act of walking down the street may become interpreted as something very different in the future. At no point has consent been given by an individual entering a public space. At most, they are warned that they are being watched, if at all, if there are signs around. Basically the message is: we are watching you, do not misbehave. It is an incredibly negative and critical message to be sending out to any citizen, it seems to me. The idea that at some point in the future somebody could say, "Right, this person wants to stand for public office. Let us Google them to see what is available in the past. Let us run some of these softwares and say, 'See the way this politician walks—completely dishonest, and we know this from gait recognition technology. Why are they over there? What is going on?' " I can see parties that would be interested in doing that sort of negative take on a person's past, either a party or the press or the media.

Q262 Gary Streeter: What is the solution to then? Is it not to take the pictures in the first place?

Dr Forbes: I do not think you can stop taking the pictures. They are there now. The cameras are there. If you think about health and safety legislation, more or less everybody is asked to do a risk assessment on what is happening in a particular situation and you get a proliferation of warnings and signs and a lot more awareness of what your behaviour might end up as or the harm that might come to you. I would have thought you need more signs saying, "You have come into this area and we are going to have your record and we are going to do what with it". I would like to know if it is going to be stored and where, how and who gets access to it. The other side of it is to say: let us think about this in a positive way instead of in a negative way. What might I want to know about what happens in my public space that I enter into and go out of on a daily or weekly basis? I would like to have access to see what is happening. I also would like to know why people are watching this. What is the use value of watching that space? What is their justification for it? What are their reasons and what are they looking for? Mostly they are looking for bad behaviour but the community might want to ask: when we are surveilling this piece of public space, let us think not about justice and crime issues, security issues, but about care issues. Might we look at this much in the way that the NHS does and say: we are not looking for behaviour; we are not looking for an individual who might be criminal, but we are looking for things that happen to the detriment of society. We might say that there is a problem here for this group of people. It is hard for them to get around; they are not serviced by the way this space is configured. There are lots of ways we can think about how we care for ourselves in our community by looking at what we capture on our images, on our webcams.

Q263 Gary Streeter: This is what you mean by new and socially beneficial uses of surveillance technologies. Does that not mean that basically more people will be looking at these images so that there is even more of an invasion of privacy?

Dr Forbes: Then the people might say, "Let's not look there". We might say that we want this camera a bit further away. We can see the benefit of watching this area but we do not see the point of intrusive watching. We might say, "Let's have some information of a different kind collected. When do we need lights on or not need lights on?" There are all sorts of things. You do not really know. The community is being watched all the time but we do not get to say from our perspective that something else might be done. There is no opportunity for creativity and innovation coming from people. The technology is there. It is a bit like text messages. The techies did not design texting for us. People decided that it was quite handy and they used it, and it became prolific and ubiquitous. We have already got the surveillance which is ubiquitous but the uses of it are not in our possession, even though it is always of us in our public space.

Q264 Chairman: Can I be clear here that what you are suggesting is that communities should be invited to come up with ideas about how community-based surveillance should take place. You are not suggesting, or are you, that every member of the community should have the same access to the cameras and televisions pictures as, for example, the people who working in the CCTV control centre would, who are sackable, dismissable, prosecutable should they breach regulations?

Dr Forbes: Why not introduce reciprocity? If you can see me without my consent, then I think I ought to be able to see what you are watching.

Q265 Chairman: One reason might be that I am happy for the images to be looked at by somebody who has been through a reasonable recruitment process, who is properly managed, who will be sacked if he breaches it and, as we have seen in a tiny handful of cases, actually prosecuted, whereas my next-door neighbour may just be a nosey parker and the last thing I want them to do is keep an eye on who is walking the street with whom.

Dr Forbes: They probably do that anyway by looking out of the window! I want to shift the balance here really. There is a dilemma of privacy and security but there are not any other creative possibilities going on of care, concern and interest of people saying, "Actually we do not want it". There is no opportunity for that. I just think (a) that people should always be consulted before cameras are set up and they should be asked why and how and contribute to that; and (b), yes, let them see what is going on, let them be bored, if they like, as well and see what happens.

Q266 Gwyn Prosser: Dr Forbes, I want to ask you about privacy impact assessments. The Information Commissioner came before the committee and he described them as nothing much more than a discipline and a risk management tool and he seemed quite keen on them. You seem to conclude that risk impact assessments might actually work against privacy, which seems counter-intuitive. Can you give us the grounds for that view?
Dr Forbes: First, if there were risk impact assessments, I would not have a problem with that but they do not say that. They call them privacy impact assessments. I have not seen one that says, "This will impact upon your privacy in the following way". They all seem to say, "This will not affect your privacy because we have terrific systems which never fail and, in any case, if they do, we will fix it almost straight away".

Q267 Gwyn Prosser: We have heard a little of that from our other two witnesses this morning.
Dr Forbes: No, I do not think that is the case at all.

Q268 Gwyn Prosser: This is a system with treble locks which will not affect privacy.
Dr Forbes: Yes, and it is about protecting that privacy, which is assumed to exist, so there is not really a discussion about what privacy is in the first place and is it privacy to me as an individual or a member of a family or a group or a profession or career? None of those things are clear and so I do not see how you can actually do a privacy impact statement unless you are clear about what the privacy is supposed to be. Mostly they seem to be compliance statements or best practice statements. I do not think any of them actually say, "This is your privacy and this is how it will impact upon it for good or ill". If they did, that might be interesting, but they do not.

Q269 Gwyn Prosser: You have nothing positive to say about their possible introduction at all?
Dr Forbes: No, because I think they are mis-named and they give you the impression that they are looking after your privacy but they do not do anything about that at all. If I want to know how good a system is, please tell me how good your system is for managing data.

Q270 Gwyn Prosser: Would it help with regards to some public assurance to assure the public that the impact has been considered, the risks of privacy would be considered if the system was put in place? Would that be possible?
Dr Forbes: I would like to see a consultation on what people think is private and what needs to be kept private. Most of them just conform to the legislation, it seems to me. You want to introduce some legislation that says: this is privacy, this is what it means, this is how it might be damaged, and do a check list that way. Then it might be interesting, but at the moment I think they are misleading.

Q271 Gwyn Prosser: Can you tell us anything about the experiences in the States and in New Zealand and Canada for instance where they are already in place to a degree?
Dr Forbes: They all seem to be the same. They are about compliance. I read the Homeland Security one yesterday and it was a joke really because it basically said, "We have a very good system and these are the three ways we protect our data and they trust us. If it breaks, we will fix it pretty soon"—if you find out, but you cannot find out. You cannot be compensated. If we think back to the popular environmental impact assessments, the evidence is that 90% of the time they do not really have an impact on outcomes. They have got to be able to say: yes, no, or do not know. If they say "yes" they are accepted pretty much. If they say "no", they might have an impact but mostly they do not. That is what I worry about with privacy impact assessments. If somebody really did say, "Look, this is going to affect our privacy", and I do not know who is going to do them, usually it is in-house, then it is doubtful that anything would change.

Q272 Patrick Mercer: Turning now, if we may, to profiling, to all of you, what particular problems are associated in your view with predictive profiling to target deviant or unusual behaviour?
Dr Forbes: The key problem here is that there is a shift that is often unacknowledged but is crucial from a person's behaviour to the identification of that person as something. I might see your behaviour but that does not mean I understand who you are or know who you are. Criminal activity does not mean that person is a criminal. They are a person engaging in criminal activity but the shift from one to the other is very quickly made once you go for predictive profiling. A person comes before you. They are scanned through your profiling system and then they are labelled. They are labelled, not their behaviour. They are labelled. That is the problem. They are then treated as if they are equivalent to that label. It is just as lazy as stereotyping. You need cohorts and you need to understand your data, but it is a way of using new stereotypes.

Q273 Patrick Mercer: What can we do about it?
Dr Forbes: I think that information is crucial. If somebody wants to gather my data and work up a profile of me, I need to know that. That would impact on my privacy. That I would like to know

about in a privacy impact statement. This data is going to be used to profile me. That would impact on my privacy because I would not really know what was going on. I do not know the routines. If you think way back to the St George's Medical School, it had a fantastic points system for admitting students until somebody realised that if you had the lowest number of points, you got in but if you were a woman you got an extra 10 points; if you were an ethnic minority person, you got an extra 10 points, just because it was in the system. So perfectly reasonable people who were not wanting to discriminate were running this system and producing discriminatory results. You do not always know what is going into those assumptions that construct the profile and you cannot really be sure what is coming out. Most of this stuff is done by companies for their convenience and for their maximisation. It is not really a public interest profiling that we are talking about to which you might agree.

Q274 Patrick Mercer: Do you accept that profiling may have a legitimate part to play in crime fighting, counter-terrorism or to enable the police effort to be concentrated in the most effective way?
Dr Forbes: Yes, but it is full of dilemmas, is it not? Yes, you want them to target their efforts. However, past experience shows that the targeting of the efforts often turns out to be discriminatory in practice on the ground, so that its use is complicated. It may well be that there was more crime amongst a certain group but why is that? It may be because that group is already targeted and more crimes were picked up. There was a report recently that shows how much middle class crime there is, which is just not picked up. Why is not the profiling targeting all these middle class criminals?

Q275 Patrick Mercer: Could NHS patient records, for instance of psychiatric patients, not be of assistance to the police in allowing them to profile people who potentially pose a threat to the public?
Dr Forbes: I think that sort of data is so difficult to get right that I would be very concerned about that.
Professor Wessely: I never thought that I would even discuss this but 20 years ago I did my PhD on the prediction of violent behaviour in people with schizophrenia. The problem is that it is incredibly inaccurate. It is okay for a large group of people and so you can make predictions about large samples in populations, but when it comes to the individual, it is incredibly inaccurate. The risk of hazard and detriment to that individual being deprived of their liberty for things that they are not going to do is very high as opposed to the one person who is going to commit a serious offence. Back when I did the research, you would be locking up something like 30 people who were not going to commit a serious crime—and this is for schizophrenia—for one who was, and I do not think it has changed that much. I am not up to date. The second point is: I cannot see any circumstances in which the police would be allowed access to, of all things, mental health records. Of all the things that are sensitive personal information, speaking as a consultant psychiatrist, that would not happen. The only way that it would happen would be through a court order, which already we would have to obey but it would be fought tooth and nail. It would be so destructive to how you deal with psychiatric patients and how you manage mental health services, it would just be quite an appalling future. I have not heard that proposal.
Professor Dezateaux: In fact it might be helpful if the police were to come and talk to epidemiologists, because they do know quite a lot about associations being a fallacy in terms of individual predictions.

Q276 Chairman: Professor, that is one of the areas we said we might question you about, but you are a child health expert. The Government is constructing a database of children apparently, and one of the aims is some sort of predictive profiling to recognise children who are seen to have a bigger set of risk factors. Can I ask you what your view is about that? Do you share the general concern about the inaccuracies of profiling or, given there are so many cases where children have slipped through the net through the failure to share information between different professions, and so on, is there actually a value in that database that is being created?
Professor Dezateaux: Yes, firstly, I do believe there is, but I think you need to make the distinction between how it allows you to deliver effective care to an individual child and avoid some of the Climbié, and so on, tragedies that we see repeatedly and stepping back and saying: how does that information at a group level, at a population level, help you in other ways? If we take, first of all, the opportunities to identify whether there have been concerns about a child, we know that quite a few children do end up in contact with healthcare before they are harmed and that it is at the moment very difficult for anyone to get access to information that would help them know that there had been any concern. Because people are conservative, there are often many more concerns expressed about a child than there would be things that would be in the public domain, even being registered at risk. So I think this information can be useful and it obviously needs to be accurate, and, again, it needs to link across a unique identifier to avoid children being incorrectly identified. I think the same point is evident, that just because certain factors are associated with an increased likelihood of a behaviour, it does not mean that just because they are present in an individual that they are behaving in this way, and I think that healthcare people need to be aware of that, but I think in terms of Every Child Matters, child protection issues that are terribly important, this is an advance.

Q277 Chairman: One final question, if I may. I want to go back to the concept that you floated and then moved on to about community assent as an alternative to individual decision-making about this. Dr Forbes has perhaps floated one model or one approach to be used in relation to CCTV, but could you say briefly what you have in mind? We can say we have all been elected by communities and,

therefore, if we all say it is all right, that is community assent, but I do not think many of us would push that out too far with our constituents. If the focus on individual control of data is not quite the right one, how would you express this community assent?

Professor Dezateaux: I think there are certain types of activity that are a class of activity where one can actually debate the principle of that and come to a position for an infrastructure with checks and balances that would be acceptable. Currently, as it is, we do not actually have a process that engages the public. So, I think that trust is very important but I think that Onora O'Neill has shown very clearly that trust that relies upon this individual consent, whenever studies have been done, show that actually informed consent is an ideal that is very, very hard to achieve at an individual level and that, in fact, you may have a better process by using community assent. However, I think it needs public engagement, accountability, communication and transparency in the systems. I think that happens within some of our ethics committees and related processes, but I think that it needs to be perhaps much more explicit in our system so that people are aware that, if they can go and visit their doctor and talk confidentially, that their data can also visit me as a researcher and will be treated with exactly the same respect as they would get from their GP.

Chairman: Thank you. Can I thank all three of you. That is an enormously helpful session. It gives us a great deal to think about. Thank you very much indeed.

Witnesses: **Dr Chris Pounder**, Editor, Data Protection and Privacy Practice, **Dr Eric Metcalfe**, Director of Human Rights Policy, JUSTICE, **Ms Shami Chakrabarti,** Director, and **Mr Jago Russell**, Policy Officer, Liberty, gave evidence.

Q278 Chairman: Good morning. Thank you very much indeed. I know that you have largely, most of you, been able to hear the previous session, or most of it. Thank you very much indeed for coming to this session on "A Surveillance Society?". I think you have all given evidence to the Select Committee in the past, but if each of you could introduce yourselves for the record.

Mr Russell: I am Jago Russell, policy officer at Liberty.

Ms Chakrabarti: Shami Chakrabarti, Director of Liberty.

Dr Metcalfe: Eric Metcalfe, Director of Human Rights Policy at JUSTICE.

Dr Pounder: Dr Chris Pounder, Editor, Data Protection and Privacy Practice.

Q279 Chairman: Can I start by asking perhaps Liberty and JUSTICE to be as precise as you can about what you see from a civil libertarian point of view as the real practical risks for individuals of the sort of surveillance society that has been conjured up by the Information Commissioner and which was responsible for us having this inquiry?

Ms Chakrabarti: It is a wonderful phrase, is it not, "surveillance society"? If it has got us all talking about the issue, and it has got your Committee engaged, then that is a really good thing, because our concern would be that, alongside other very important societal concerns, like security, like public health, as we have heard, sometimes the value of personal privacy can be lost. There are very good reasons why that value can be lost and forgotten on occasion. Of course, by definition, privacy is a qualified right, unlike some of the rights that Liberty and JUSTICE defend sometimes—the right not to be tortured, the right not to be arbitrarily detained. Privacy, by definition, is a qualified right. We know that we are social creatures. The moment we come together, even in very primitive societies, or when we come together in families, let alone complex modern societies, we do give up a little bit of varying degrees of personal privacy, sometimes voluntarily and sometimes not voluntarily, but in a way that is, of course, necessary and proportionate in that society. The danger is that, because it is a qualified right for the individual, but also, I would argue, some of it is very important to society more generally, to the flavour of democratic society, if we are not quite rigorous enough about the defence of something that is about balancing that right against other great concerns like security, health and so on, we can, without really noticing and without having proper public debate perhaps, lose very important things from democratic society. For example, without really quite a significant degree of value paid to personal privacy, there would be a society where the dignity of the individual has been compromised; intimacy between people, confidence between people and trust in big institutions, whether it is the Health Service or the Government, would be lost. Where we are, I would argue (and I think Mr Thomas would agree), perhaps Britain in 2007 is at a place where there are great technological opportunities to interfere with privacy, often for very good reasons, and we just need to make sure that the ethical, political and legal debate keeps apace with all of this technological development.

Q280 Chairman: Moving on to you, Dr Metcalfe, can I perhaps put the question this way. Should my concern be that somebody will actually find out something about me and do something to me as a result, if you took Dr Forbes, the previous witness, that all my neighbours can watch the CCTV as well as the CCTV control room, or somebody finds out something about by credit record or something and damages me, or is it almost a more philosophical objection that some people would say, "Even if nobody does anything to harm me, I have somehow lost out as a free citizen by the fact that other people have got access to information about me that I

would rather they did not have"? Where in our inquiry should we be focusing on the practical damage that can be done to individuals or the philosophical concern that we are less free if other people have our private information?

Dr Metcalfe: I am sorry to say that you have to focus on both. It is entirely true that you have to focus on the practical, but also, yes, you are harmed, in a way, if the information is stored, even if the information is never actually seen by anyone else, because your own sense of personal privacy is affected by the knowledge that people have access. For example, if I write a diary and I leave it in a room and I am subsequently aware that maybe 10 people have gone through that room and had the opportunity to read my personal thoughts sitting on the desk, maybe none of them did, but already that has had an effect on my personal privacy. If you think about all your personal data as being in that diary and if you think about not merely 10 people passing through that room but, say, all the relevant agencies that have come on to the stage having access, then you have reason to be concerned, and your own sense of personal privacy, which we think has a very important value because it allows us to do so many things that we take for granted as being part of a good life, is affected as a result. There is a chilling effect that comes about in that kind of situation.

Chairman: When you talk about your diary, I feel very much the same about my blog. Anybody could read it, but nobody seems to bother!

Q281 Mrs Cryer: Shami, congratulations on your CBE. I just want to take it a bit further from what the Chairman has been saying. I want to ask you all if you accept that there could be real and pressing needs for data sharing, particularly in the light of what happened on 7/7 two years ago and given the fact that we all recognise that the most precious human right is the right to life itself and to keep our bodies intact. Therefore, how do you compare that need for the public to know what is going on and protect our citizens with the overriding consideration for individual privacy?

Ms Chakrabarti: I think you have to do it on a case by case or policy by policy basis. I think that the principles in the European Convention, and in this country they are older—there is the justificatory principle for interfering with the individual—still work very well. So, rather than balancing these issues at an abstract philosophical level, we would look at a particular policy, or a particular interference, a particular need to match data or to access data. I am assuming you are talking about the law enforcement context or the investigation context possibly by compulsion rather than voluntarily, though in other contexts sometimes voluntary sharing is good enough. You say, "Is this policy, is this measure, is this particular accessing of data truly necessary and proportionate for this?" and it is balance. That is why it is so difficult. If I may say so, that is why Parliament is actually better suited to protecting privacy (and I think it has got a long way to go) and I hope this is the start of it, than the courts are. In my experience the courts are almost uniquely well qualified for dealing with a situation where what is at stake for the individual is torture or incarceration, and that is being balanced against other factors, but the courts are not best placed where the balance is between two great societal objectives, where the interference with the individual's right is not that great actually. Some would argue that if my DNA is taken from me, for example, when I am arrested for shop-lifting, even though they got the wrong woman and the police apologised to me and sent me on my way, the DNA is now kept forever because someone says one day I might be a terrorist or I might be guilty of shop-lifting, the courts have not so far been very good at conducting that proportionality exercise, but I would hope that because that taking of DNA is as much an issue for hundreds and thousands of people as it is for me individually that Parliament is actually much better suited, and in the future I hope that the debate about privacy and various policies could be really enhanced by greater Parliamentary involvement.

Q282 Mrs Cryer: Would anyone else like to comment?

Dr Pounder: Just one comment in relation to trust and trusting in the data sharing arrangements. I think the issue is one of trust, and possibly the risk is the global erosion of trust. The previous speaker, Professor Wessley, said in relation to medical research there was a lack of trust in the system, and that he had experience in people refusing to give consent for medical research. If you look at the data sharing arrangements, all the trusting is from the public. The public has to trust that the data sharing is limited in accordance with the rules, the public have to trust that staff who do the data sharing are properly trained and follow the rules, the public have to trust that the procedures for authorising the data sharing are properly maintained and the public have to trust that Parliament does not enact legislation that provides for function creep. All this trusting is in one direction. What there needs to be, as Shami said, is a strong counterbalance to that public trust. All the trust is coming from the public to the authorities with very little counterbalance, in my view.

Ms Chakrabarti: Ironically it could manifest itself. If this trust is broken on occasions or generally, it manifests itself, not just in a way that is of detriment to the individual but of great harm to public policy as well. For argument's sake, if there were a health collection of data, and, of course, we have heard from people who care about protecting trust and privacy, your previous witnesses, but if you got to a point where the public no longer trusted the protection of their confidential information that they share with their doctor, people would say less to their doctor, and then, suddenly, you have got a counterproductive policy where you thought you were being so expedient by saying more and more people within the Health Service, etcetera, etcetera, can have access to this data because we are going to do such great research and we are going to help people wherever they are in the country. That all

seems very laudable, but if you lose trust, then the woman who has been battered does not confide in her doctor any more. So, it is this very difficult balancing exercise which, as Dr Pounder has said, can also be enhanced by saying information is taken for a specific purpose. We put more robust ethics and laws and practice and culture in place to make sure that there is not just a general free-for-all or a general presumption of sharing where it is it expedient rather than sharing when it is truly necessary and proportionate.

Dr Pounder: Can I add.

Chairman: No, I am sorry, to get through the questions, we have got four witnesses, we cannot have everybody having two goes at every answer, so if everybody can be brief and if people have said the main points, please can we move on.

Q283 Mrs Cryer: We were talking mainly about public authorities and their knowledge of people. Can we move on to private authorities, private concerns, and their accessing and holding information on individuals and, even more complicated, where the functions are contracted out from public authorities to private authorities. Would you comment on those areas about access to private information?

Mr Russell: I think there are a number of similarities and a number of differences between large databases held by private bodies and large databases held by public bodies. Liberty has concerns or is interested in both but has mainly focused on public bodies, it has to be said. For example, in the context of our concerns about CCTV, that applies both to private bodies and public bodies. I think one of the main differences is this question of consent. In terms of giving information to a private body, it is very much based on consent but actually, in the context of providing information to a public body, it is often compulsory or, if it is not compulsory, it is basically, in order to receive a public service which people are paying for by their taxes, you have to provide that information. I think that is quite a key difference between these two types of database, but, of course, there is a big question as well about informed consent in terms of providing information to private databases and whether people are really aware about the value of what they are providing to those kinds of companies.

Dr Metcalfe: I think there is a significant problem with private companies in that they are not always motivated by the same issues as the public sector obviously. In fact we received a letter very recently about the use of fingerprinting technology being sold to schools. A number of private security companies are selling schools security systems, whereas you used to be able to access the school library by way of a library card, and, indeed, with school lunches you now can have a fingerprint system. The kids just swipe their fingerprint across a scanner and that is matched against a record of their fingerprints, which are stored. So, you now have private companies holding fingerprint databases of school children. There are, obviously, various legal measures which can apply to that kind of situation, but I think it is a very good example of the way in which technological change is impacting upon personal privacy without very much appreciation of that impact.

Q284 Chairman: It has been suggested to us that public sector companies are being covered by the ECHR, private sector companies are not being covered by it, and that possibly, going by the recent court ruling last week, for example, if the DWP at some point contracted out its work on investigating incapacity benefit to a private contractor, the private contractor would not be covered by the ECHR provisions. Is that correct, and is that a significant issue to worry about?

Ms Chakrabarti: Sadly, it is not completely clear. What is clear from, in my view, a very disappointing decision last week is that residential care homes have not been considered to be public authorities, regardless of Parliamentary intention or the vulnerability of the people concerned. The case is confined to that situation, and their Lordships did try to distinguish a number of other potential scenarios, but there is a lack of clarity. You would not be able to say that all public functions that are contracted out are definitely caught; and so there will be parliamentary work to be done. I would argue, on a sector specific basis to be absolutely certain, that where Parliament is allowing local government or central government to contract out a particular service, that Parliament makes the decision, at the time of providing that sector specific legislation, whether it intends the Convention to apply, because I do think it could be an important safeguard.

Mr Russell: Can I give you an example of where this particular issue is arising in a bill that is before Parliament at the moment? It is the Serious Crime Bill, and there is a power in there for the Audit Commission to mine data in order to identify potential fraudsters. There is a power in that bill for the Audit Commission to subcontract the power to do that data-mining, this kind of mechanical, computerised fishing expedition, to a subcontractor, to a private body. I think what was said is that, given the doubt in the court's mind about whether that body would be covered by the Human Rights Act, Parliament could clarify in the Serious Crime Bill that, for the avoidance of doubt, any private contractor will be covered.

Dr Pounder: Could I quickly add on this point. The Data Protection Act has its concept of a data controller. The data controller is the person who has the statutory duty and if somebody contracts out delivery of the statutory duty, the delivery of service to a data processor, I think the data controller would still be in control of the data. That is my own view of it.

Chairman: That is a very useful comment. We can rehearse current issues around it.

Q285 Ms Buck: Can we pursue this issue of the difference between the approach of the private sector and the public sector, and just to ask, particularly Dr

Pounder, but others may have a view, about what could be done. If we assume that the consent element in the private sector is a strength in terms of data protection, what could be done within the public sector systems to, if not exactly follow down that line, perhaps for some of the reasons we heard from the earlier witness, to try as much as possible to build in that kind of informed consent? What would be the systems requirements and how feasible is it?

Dr Pounder: It depends on what you are doing. The previous witnesses said something about the police and consent which personally I did not think was quite right. I cannot see the police seeking consent for anything. If you have a statutory duty you do not need to seek consent, end of argument. What you can build in, in certain circumstances, is the right to object to the processing of personal data. So, in the private sector body, say, for example, I do not like Tesco. I have consented to Tesco processing my personal data. I am able to withdraw consent quite easily, for example, in relation to marketing or, possibly, in relation to their databases that look into my sales and purchases. So, for some areas of data sharing in the public sector, where there is a statutory gateway that permits the sharing but the sharing does not involve, say, for example, law enforcement, that kind of area, you could have an easy right to object to the processing. When the UK Government implemented the right to object in the Directive they implemented it in the narrowest possible terms, and that could be broadened. I am thinking particularly, for example, of the facilities in the identity card legislation that allows for disclosures for efficient and effective delivery of public services. You could have a right to object there.

Q286 Ms Buck: Having listened to those witnesses, particularly on health, to what extent do you accept that there is a tension between public good, in terms, for example, of the benefits of using accurate epidemiological data, and the kind of protection and the potential right to opt out or to change data?

Dr Metcalfe: I think a very good example is the police DNA database, because we have already seen applications being made by medical researchers to use that information; and it is all very well to say that the information is being stored for one particular law enforcement purpose but, as we know, the definition can go very broadly, and so you might say that the storing of DNA for a law enforcement purpose means that it should only ever be used in relation to a specific crime and a specific forensic investigation, but what we find happening is that medical researchers will go along to the police database and say, "We are interested in the idea of perhaps a gene for criminals. Can we do the speculative search in relation to your database to see if there is a link between, say, for example, people with red hair and criminal behaviour and potentially, given the breadth of the scope of the law enforcement purpose, that could actually fall within it. Obviously the police DNA database has its own regulatory framework and there are high ethical standards in relation to medical research, but I am not going to say it is impossible. I know that medical searches have already been approved in relation to it.

Ms Chakrabarti: There comes a point, I think, where you really do need to start saying: is the Information Commissioner well-resourced enough? Does he have enough powers to really police even the existing Data Protection Act, and you have to say, given all the possibilities that we have at the moment and which are coming, Parliament is going to have to take a more robust role because there is a tension, there will be a tension at times, and I am not going to say that the previous witnesses are all wrong about the enormous potential benefits, but someone has got to make that judgment. When they say the normal paradigm has been consent or anonymity but that paradigm has to change, I would argue that it is you and your colleagues who should be conducting that judgment ultimately on behalf of your constituents, and, frankly, if that kind of paradigm is going to be ignored on occasion because they are going to cure cancer, then I think maybe there should be a specific bill and there should be a robust parliamentary debate. Generally speaking, law enforcement and the state have powers of compulsion, but in return there has been greater accountability. That is generally the trade-off. The private sector has generally been taking information by consent and there is less accountability. The lines between the private and public sector are increasingly merging to the point where I am not even sure the distinction is that helpful. The real question is the purpose for which the interference is taking place, who sanctions the interference and what are the protections against abuse?

Q287 Ms Buck: A last question on that really, which is, I think, particularly for Dr Pounder. What about the scope for actually changing and adding to data in a way that is theoretically possible, although I suspect in practice it is not quite as easy as that, to change data on your credit rating? To what extent should it be possible within public databases to actually amend and correct data?

Dr Pounder: There is specific legislation (the Consumer Credit Act) that permits that. In relation to the NHS discussion that we had, the NHS Act 2006 allows the disclosure of medical records without patient consent, subject to the Patient Information Advisory Group giving permission. I was a bit puzzled about why the medical researchers do not use the statutory routes that are available to them. In relation to public and private sector merging, what I would say is if you look at, say, the credit reference agencies—that is private data—credit reference agencies collect a whole pile of transactions from the banks, the telecommunications companies providing data to the authorities on a regular basis, the public and private sector is merging—. The barrier is not there in large databases. I think Shami is right, you have got to treat the whole thing case by case.

Q288 Mr Winnick: Liberty and JUSTICE, in particular, the paper we received from Liberty, paragraph 12, the final sentence of that paragraph states, "There is growing public unease about the extent of the surveillance society." What evidence do you have of such public unease?
Ms Chakrabarti: I am going to call on Mr Russell to answer that, but can I apologise at the outset for the author of this evidence not being here. Gareth Crossman is our privacy expert, he will publish a report later in the year, but I am afraid that the rights of privacy and family life seem to allow people to take personal holidays when they are working at Liberty. I did take advice on this.
Chairman: We will hold you collectively to the evidence, I am sure.

Q289 Mr Winnick: Mr Russell what evidence do you have?
Mr Russell: First of all the anecdotal evidence is that we do receive hundreds and hundreds of queries from the press, and I suspect that you receive hundreds of letters through your mail bags about privacy type issues, but it is definitely something that we receive a lot of mail on.

Q290 Mr Winnick: Mr Russell, can I interrupt you. I do not know about my colleagues; I cannot recall in recent times a single letter from constituents complaining about lack of privacy. I am being the devil's advocate, because to a large extent, as often with Liberty and JUSTICE, I intend to take the same view as you, but my job, like my colleagues, is to cross-examine you and find evidence for your statements. When you say there is great unease, that everyone is trembling in our constituencies that their privacy is being invaded, pray, give us some evidence.
Mr Russell: There has been some limited polling done on this, and there was an article at the end of last year in the Telegraph with some YouGov Survey and that said that 78% of people felt that they lived in a surveillance society. Only 2% thought, for example, that the Government could be trusted to run an ID card scheme which did not contain serious errors. Fifty-two per cent were fairly unhappy, or very unhappy, at the idea that personal data could be recorded on government databases. So there is some data. One of the things that we will propose and will consider in this report to be published later in the year is the idea that more polling needs to be done, more information needs to be done about public attitudes to surveillance, but there is some suggestion in this limited data that there are public concerns.

Q291 Mr Winnick: I am going to ask you this question, Mr Russell. If there is such concern, why is it that, not only perhaps my colleagues have a different sort of post bag, but if I have not received such correspondence and my constituents, certainly those who write letters, are not usually reluctant to express their point of view, I get quite number of letters of a different kind asking, in fact, for CCTV cameras. Of course they take the view (perhaps it is exaggerated) that CCTV cameras, in the view, presumably, of the large majority of people in this country, play some part in undermining criminality. If there is such a feeling of concern, why do I receive letters along the lines I have just indicated?
Ms Chakrabarti: In my experience it is extremely dangerous for Liberty to fall into the trap that you are setting, which would be to suggest that general elections are going to be won or lost on CCTV. We are not in a position to argue that. Of the issues that people write to us about, that is already a more limited class. People do not ask us to build a Health Service for them, etcetera. It does seem to be a very high concern. When MPs write to us, which they do as well, to ask for help, on many occasions they are writing to us with concerns about fingerprinting in schools, DNA and so on. It may be a healthy minority of the public. I do not think that there is going to be a revolution about CCTV, but CCTV is really interesting. There is an interesting cultural point if you compare Britain to other European countries, because even in as far as privacy interferences go, there are big cultural differences about which particular interference people are concerned about. In Germany or other parts of the Continent you put a CCTV camera in the wrong place and there literally will be riots, and may be that is the non-democratic past. As a result, the authorities go through a much more rigorous process of community consultation and analysis before they decide where to place cameras. They put them up for the October Fest in Munich because they are expecting anti-social behaviour and trouble. At the end of the festival they take the cameras down. In Britain we seem to have had a much higher tolerance of lots and lots of cameras that seem to make a lot of people comfortable, but we still have concerns that from an efficacy point of view having lots of cameras everywhere, many of them not particularly well looked at or maintained, is not necessarily the best use of public money but also it is largely unregulated. Mr Denham made the point that you would feel better about the cameras if you thought that the people who were operating them were properly trained and properly recruited. That is not always the case, and it is not really regulated as an industry. I am not going to sit here and say that every single CCTV camera that has ever been erected is a complete violation of human rights, but I do think proportionality has a lot to contribute.

Q292 Mr Winnick: Next time I receive letters about that I will bear in mind your comments. Dr Metcalfe, do you believe on behalf of JUSTICE that there is a large feeling in the country that we are on the verge of 1984, big brother and the rest?
Dr Metcalfe: I think there is public unease. I do not think there is enough. There should be more public unease.

Q293 Mr Winnick: There should be more, but it does not exist at the moment.
Dr Metcalfe: There is public unease. We get the same letters and emails and telephone calls that Liberty get inviting us to take up concerns. Generally

speaking, we go along, we have our club card points, we have our credit cards, we walk along the street, we are monitored by CCTV and we really do not think about the impact these things have on our personal privacy. Maybe someone is arrested. It is a case of mistaken identity, but someone makes a complaint about them being, say, a sex offender. They are acquitted or maybe charges are not even brought, and they think nothing of it until the next time they try to apply for a job working with children, and then they find they cannot because they have failed the child protection check because of the fact they have been arrested in relation to a sex offence means that that information has to be disclosed. That is the point at which people recognise that personal privacy has some importance. I am not saying for a moment that that kind of information should not be disclosed, I am saying that we do not have very much appreciation of the way in which information is transferred, even with our consent, because we all tick the box on the credit card form, not being aware that it says, "This information may be transferred and shared with other third parties", but we never fully appreciate, until we start receiving marketing letters from other people on the credit card list, how precisely that information is being used. So there is public unease—a lot of issues, like, for example, fingerprinting in schools that came to our attention by way of a letter—but is there enough? No, there is not.

Q294 Mr Winnick: Can I put this question to Dr Pounder. Is there a contradiction between what we were just dealing with, the concern and how far it is extended regarding intrusion into private lives, and the fact that an increasing number of the public seem to take what could be described as a remarkable casual attitude to publishing large amounts of personal data about themselves? For example, FaceBook or MySpace websites. For all we know, on Mr Denham's blog he might be openly speculating what sort of job he is likely to be offered later this week!

Dr Pounder: People have their own view of privacy. Lots of people are ex-directory; lots of people are not ex-directory. Some people when they fill out an application form tick the box before filling in the form. If people want to put their personal information on the Internet, then, basically, that is them giving permission, but coming back to the point here—

Q295 Mr Winnick: Pursuing that for a moment, it does demonstrate—I do not do it myself—the fact that there seem to be so many people, perhaps younger people, putting such information on the websites which I have mentioned. It does not seem me to express a fear that their personal privacy is in some way being invaded.

Dr Pounder: Well, they take the risk. Whether they know the risks, I do not know, but coming back to the point here—seriously, it has to be faced—there have been 20,000 complaints to the Information Commissioner last year.

Q296 Mr Winnick: How many?

Dr Pounder: Twenty thousand in the annual report. The annual report also has a tracking survey for privacy that picks up Liberty's issues. You are already having people thinking of the "Big Opt-out" in relation to the Summary Care Record of the NHS, you have people, in a sense, questioning (and I am sure you have had this) why the police have DNA data on somebody who has not committed a crime, you have even got people questioning the electronic tag on their rubbish collection. If that is not concern about surveillance, I do not know what is.

Ms Chakrabarti: To interrupt—

Chairman: No, we are not going to have two attempts at the question. Can we move on?

Mr Winnick: I assure you, Dr Pounder, I share your view, although it might not appear to be in my question.

Chairman: Meanwhile, I am composing 10 pictures of my favourite members of the Select Committee! Carry on, Mr Winnick.

Q297 Mr Winnick: I am sure I would be foremost. Dr Metcalfe, JUSTICE, you argue that the interests of the private individual and public good are not opposed—this is the point of view you have expressed—but is not the job for parliamentarians somewhat different, a question of personal liberty versus the common good, and trying, as far as we are concerned, to reach a balance between the two?

Dr Metcalfe: The point I was trying to make, and it was probably the most philosophical section of our evidence, is that personal liberty is ultimately part of the common good, that we benefit from having privacy, we benefit not merely as individuals in having privacy, we benefit as a society: because people do things in their private space, in their private time, and the benefits from that flow on to society as a whole. You could give the example of a writer. We would not have much of the great literature that we have today if, say, all our great writers thought that everything that they wrote down was likely to be under surveillance, for example. It was just a very abstract philosophical point about the way in which privacy exists, not only for the individual, but also for the common good, and that we should be very careful about the impact of new technologies that threaten that, and I think MySpace and FaceBook are very good examples. It is great that we have these new communication networks, but I do not actually think that lot of young people think very clearly ahead about the way in which their personal data could be disclosed and could be used, in the same way that young people do not think ahead about an awful lot of things, like their educational choices and how much they drink on a Friday night. So, in the position of responsibility that Parliament is in, we need to establish greater safeguards to ensure that other bodies, other agencies, other companies take responsibility as well.

Q298 Mr Winnick: Presumably that is Liberty's point of view?

Ms Chakrabarti: Absolutely. You were all elected in secret ballots and the concept of a secret ballot is essential to free elections. Without this right, even in the human rights community, sometimes regarded as a bit low-level, a bit trivial—it is not torture, it is not arbitrary detention—you cannot have free elections, freedom of thought, conscience and religion, freedom of speech in some circumstances without that little bit of personal space and respect for it. I completely agree with Eric on the young people and the FaceBook point. The threats do not just come from the Government or big business; if we are not careful we will rear a generation of young people who have not really known the value of privacy as part of dignity, as part of respect. People can take pictures of each other with their mobile phones; they put pictures of their girlfriends on Internet in states of undress. We as citizens, if you do not help us to resurrect the importance of privacy and dignity, could be a great enemy to each other in relation to this value.

Q299 Patrick Mercer: Turning now to automated data exchange and Shami Chakrabarti, this is for you, please: do you think that the creation of databases sometimes provides an easy or a lazy solution to problems that actually require better communication and co-ordination between responsible professionals?
Ms Chakrabarti: Yes, I do. That is a very helpful and leading question, but, yes, I do. At Liberty we try to take a balanced view of these issues. We are not against all databases, how could we be, let alone all automated databases, but sometimes, we would argue, when something bad happens it is easy to say that the answer, for example, to a Climbié situation is to build an ever bigger database, whereas in the specific tragic case of Victoria Climbié it was not the lack of a data entry of every child in the country, a lot of bad things happened to that girl before she came to her tragic end and people did not communicate about the specific. Obviously, sometimes when you are looking for a needle in a haystack, it has been said many times before, do not build an ever bigger haystack where you increase the risks of accidents, and so on and so forth.

Q300 Patrick Mercer: I am referring exactly to that sort of case. Do you think there is a real danger that a focus on automated data-sharing can actually make getting across essential information harder, and there is simply too much information out there? It confuses rather than helps.
Mr Russell: The thing we said on the children's index was actually, in principle, there is nothing wrong with a children's index, if it is a targeted database. Targeted amounts of information on children at risk can be helpful. The problem is, when you have got every child on a database, as Shami said, it is incredibly difficult to see the wood for the trees. In certain circumstances, yes, a database is important, but we need to be—. These human right principles that we started off with—is this necessary, is there a legitimate aim, is it going to work—those are the questions we think Parliament should be asking when a new proposal for a new government database is being proposed.
Chairman: Thank you, Margaret Moran.

Q301 Margaret Moran: I, like David, am interested in the evidence base of some of the things you have been asserting to us. You say in your submission to us that the extent to which every person in the UK is subjected to surveillance has increased disproportionately to any justified social need or benefit. Could you give us the research evidence for that just as a reference? If you cannot do it now could you, please, send it to us? You also make reference to the National DNA Database and say that there is an intention to make that database compulsory. Could you give us what evidence you have for that statement?
Ms Chakrabarti: It is, of course, compulsory even now as a matter of law, because this is a criminal justice policing measure. Your DNA is compulsorily taken from you under pain of criminal sanction if you do not agree to it being taken.

Q302 Margaret Moran: I think the suggestion is that it implies universally?
Ms Chakrabarti: That there be a desire in certain quarters to make it—

Q303 Margaret Moran: You have stated that you believe that a compulsory universal DNA database—
Ms Chakrabarti: The present, soon to be outgoing, Prime Minister has stated that he thinks it would be desirable to have a universal DNA database after a public debate. Various chief constables have taken that view. It is a perfectly respectable, if slightly terrifying, view. There is logic to it. There is a logic that says, "Let us have the DNA of every man, woman and child in the country, and then, when something bad happens and there is a crime scene, we will match it." There is also a logic, I would argue, to our position, which is to say, have a smaller more ring-fenced DNA database of people who have been convicted of a particular threshold level of crime. What there is not a logic to, in our view, is the current situation where anyone who has been arrested for an offence can have their DNA taken and even if they are let go, as in my shop-lifting example, the police apologise, say, "We have got the wrong woman", never charged, let alone convicted, my DNA can be kept forever.

Q304 Margaret Moran: I was not actually asking for a treatise on DNA, I was asking for the evidence-base?
Ms Chakrabarti: That is the evidence; that is the law.

Q305 Margaret Moran: Various comments do not constitute a research evidence base either to the initial point I made or to the second of those points. Have you got something substantial other than people's comments?

Ms Chakrabarti: Well, the legal position is clear and not in contention as to what the basis for taking and keeping people's DNA is at the moment. That is a statement of the law.

Q306 Margaret Moran: I was referring to your assertion about a universal—
Ms Chakrabarti: If the Prime Minister says he thinks it would be a good idea, I think that is a pretty good suggestion of intention, and, as I have said, it is a logical position, I just do not think it is proportionate.

Q307 Margaret Moran: Mr Russell, earlier you made reference to the Serious Crime Bill. The reason I have been out of the room is because I am sitting on the Serious Crime Bill. You referred effectively to function creep, to what is now known in technical circles as the possibility of phishing, data-mining, data-sharing. What evidence have you got for that function creep and are you aware of what the Minister said at the second reading on the Serious Crime Bill in relation to that in answer to the specific question that I raised?
Mr Russell: The specific point about function creep and where my concern about the function creep comes from is the fact that in the bill there is a very clear provision which says that the Home Secretary, Secretary of State, may by order increase the functions for which data-mining may be undertaken. So, that is how function creep most often happens: if you have got a power to do something with personal information and then, by regulation, the reasons for which you can process that information can be extended. That is where the concern about function creep comes from. There is a clear power in the bill. I cannot remember the clause reference, but there is one there which says that the purposes can be extended. So that is the function creep point.

Q308 Margaret Moran: That contradicts what the Minister said at the second reading, that the Audit Commission will not be able to use the powers to predict who might commit fraud in the future, in other words phishing, and it is right and proper that we put safeguards in place to prevent data-mining and data-phishing.
Mr Russell: Can I come back on that point? That is absolutely right. We pushed in the House of Lords for an amendment to the bill which would prevent data-mining to be used to profile people's future behaviour. The Government agreed with us that that was a concern in the current legislation and, therefore, agreed in the House of Lords to put an amendment in to stop profiling of individual suspects in terms of their future behaviour, and we are delighted they have put that in. That is slightly different to the question of function creep, because the question of function creep is about what purpose is this data-mining going to be used for, and I would be very surprised if the Minister had said that there was no risk of function creep in relation to this aspect of the Serious Crime Bill, because the provision is there.

Dr Pounder: Just a comment on the Serious Crime Bill. The Audit Commission can do data-matching in relation to serious crime, not so serious crime and debt collection. In relation to debt recovery, one wonders whether the Serious Crime Bill is the correct vehicle for this. There is a real problem in over-indebtedness in the UK. Whether or not that should be treated by separate legislation is another thing, but if you look at Schedule Seven, you will see that debt recovery is part of the Audit Commission's remit in the Serious Crime Bill.
Dr Metcalfe: Can I make an additional point about function creep. Before I was at JUSTICE I was a lawyer in the immigration and judicial review section of the Treasury Solicitors Department and I was responsible for helping to arrange advice in relation to the Asylum Registration Card or ARC, so that was an identity card system which involved fingerprinting of asylum seekers. I am not saying anything that is not in the public domain at this point. The original purpose of the Asylum Registration Card was to reduce fraud in relation to asylum seekers, but it is very easy to see, just as a practical measure, how the information stored for one purpose can be used in relation to others. If you had that information stored in relation to asylum seekers and you are a law enforcement agency, why would you not want to check information to see whether any of the people that you now have on your database match unsolved crimes? Why would you not want to see if any of those people are also involved in relation to mainstream benefit fraud, if in some way they have managed to fraudulently obtain documents in relation to mainstream benefits? Why would you not, if you were a medical researcher, want to cross-reference the biometric information that you might have on that database in relation to preventing genetic diseases? You do not have to be a conspiracy theorist to see how function creep happens. It happens perfectly naturally, in that people see information which is useful and then seek to gain it; and no-one can deny that these databases are useful; the point that we are trying to make in this situation is that what people do not see when they see the utility of information is the danger and risks. I thought the evidence this morning from the people involved in medical research was extremely interesting. Yes, it is true that in the old days you could go into a doctor's surgery and get a patient's medical records off the doctor's desk, but, generally speaking, that would mean going down to a quiet street in Basingstoke, finding the doctor's surgery and going in there. Now, anyone with a computer can access that information. Just to give you some idea of the extent to which—

Q309 Chairman: Just a minute. It is not actually true, is it, that anyone with a computer can access the NHS database? If you want to let that lie as your evidence that anyone with a computer can access the NHS database, I think you need to justify it.
Dr Metcalfe: Obviously, I am generalising to a degree. The computer has to be networked and also has to be able to access the NHS network.

Q310 Chairman: That is quite a big difference, is it not, between "anyone with a computer"?
Dr Metcalfe: We are currently extraditing a man to the United States because he was able from the United Kingdom to hack into the United States Department of Defence database. Do we really suppose—. I do not think literally everyone with a computer can access that information, but I mean anyone who skilled enough with networks, and there are a large number of people like that nowadays out there. If someone in the United Kingdom can access what is arguably the most secure defence network in the United States from here in the United Kingdom, I do not think we can afford to be blasé about the possibility that someone, say, in China could at one point hack into our NHS database.

Q311 Chairman: Nonetheless, you take our point about being a little bit more accurate.
Ms Chakrabarti: He qualified it.

Q312 Margaret Moran: The suggestion you are making there is that these other uses should not be occurring. What would you advocate to prevent phishing? Are there limitations that could be placed on the use of this data that would give sufficient assurance, in your view, to the general public or to yourselves rather, because maybe the general public have a different idea?
Dr Metcalfe: I think really it has to be taken on a case by case basis, because obviously not all databases are equal and different databases work in different ways. One major source of concern, for example, is the recent European Framework Directive, which allows law enforcement agencies from across the European Union to access information held in UK law enforcement databases, which means that information could potentially be passed from police criminal records to a law enforcement agency in Lithuania. One major concern there is what assurance do we have that the end user in Lithuania will not misuse that data, because they are not subject to the same data protection standards as we are here in the United Kingdom? I think that is a very good illustration of a potential gap. We need to make sure that every end user, every person who has access to official government data is bound by the same standards. So, that is one global point I would make, particularly in relation to data-sharing across the European Union. In relation to the specific—

Q313 Margaret Moran: I want to be clear. You are saying there should not be sharing of data across Europe or beyond until all of those protocols are in place. I think the parents of young Maddie might have a different view on that.
Dr Metcalfe: Certainly, I would hope so, but I would also like to think that they do not want her personal data being shared willy-nilly with people in another European Union country without sufficient data protection standards. Think of the potential risks, for example, if you allowed access to our children's database to be given to any accession country, and think of the potential risk to children that might arise from that situation, because we are not asking the same standards of an accession country that we do of our own public officials in this country.

Q314 Gwyn Prosser: You have all argued in your various ways that the current legislation does not provide comprehensive data protection, that it is out of date, out of step and fails to keep pace with technological changes. I wonder if I can ask you briefly each to describe revision or improvement in the legislation which would correct that error and how can we ensure that such provision does not get outpaced by the rapid improvement in technology?
Dr Pounder: I think the starting position I have is that there needs to be a counterbalance to the data surveillance and the data-sharing that occurs. I think there are three elements to this counterbalance. One is parliamentary, the second is regulatory and the third is the individual. Starting from the individual basis, I think the time has come to look at a right to information privacy. The Culture and Media Committee toyed with this idea and recommended that Parliament should grab this particular nettle. My own view is that it can be done via the Data Protection Act, a right to information privacy, and the advantage of that is that it would not disturb the relationships with the press, it would avoid that problem. In relation to parliamentary, what I would like to see is the ability to have a feedback loop into Parliament that could possibly result in, say, for example, a show-stopper in respect of, shall we say, some sort of surveillance activity potential. I will try and explain what I mean. At the moment the Home Secretary and many secretaries of state are responsible for setting the procedures that safeguard as well as the responsibilities for interference, and I would like to see Parliament being more on the ability of being able to, shall we say, have some safeguards. For example, the Home Secretary could produce a Code of Practice in relation to X and, say, for example, he could approach the Information Commissioner with a view to what the Commissioner's views are. Instead of the Code of Practice being, say, for example, laid before Parliament, it could be approved by Parliament. So, if the Information Commissioner, for example, had problems with the Code of Practice, he could bring those problems to Parliament and Parliament could set social policy as to where the balance lay. I also think that the regulator, the Data Protection Commissioner, should have the ability to check regulations passed by this House (and as you know in the identity card legislation there are some wide-ranging powers), shall we say, for example, to go straight to the court and say, "I think these regulations are awful", and have somebody who can actually challenge the lawfulness of the regulations that are placed in human rights terms. I also think Parliament needs more information about what government intends. The bulk of the appendix in my evidence relates to how I thought that Parliament was not informed as to the true intent of the identity card, and I hope that in the new arrangements, with respect to Gordon Brown's possibilities, that Parliament will be able to get the information it

seeks to make informed decisions. In relation to the regulator, the final thing I would say is that—. Sorry not the regulator. A general matter is that there has to be absolute transparency in relation to data-sharing or any surveillance, what is going on, and that absolute transparency has to be backed up by the fact that people can do something with the information. It is pointless telling you, "Oh, there is a camera here", blah, blah, blah. Once you have been given this information, you can do something, and that is one reason why I think a right to information privacy is inevitable. At least the individual who is subject to the surveillance can do something with the information that he gets.

Q315 Gwyn Prosser: Dr Metcalfe, would you concur with that?
Dr Metcalfe: I would concur with that. It is very difficult for me to add anything further. Perhaps one point I should just identify, if we are going to identify wish-lists. We would argue that there needs to be prior judicial authorisation of any interception of private communications under Part I of the Regulation of Investigatory Powers Act. Currently you can intercept, a law enforcement agency can intercept email, it can intercept telephone calls, it can intercept letters and text messages simply by going to the Home Secretary and asking for a warrant. I am not saying that the Home Secretary grants them willy-nilly, but in every other common law country you find that the prior authorisations are made by independent judicial authority. That does not happen in this country and it should.

Q316 Gwyn Prosser: Ms Chakrabarti or Mr Russell?
Mr Russell: Again, we agree with the comments that have been made, and I will not repeat them. There are another couple of points that we would make. We need to look at the Data Protection Act with specific reference to CCTV, because a large number of CCTV cameras are not regulated by the Data Protection Act at all, and we think that there should be very sensible, legally binding guidance or regulations on the question of whether people have to be informed about where a CCTV camera is, who operates the CCTV camera or what training they need and the appropriateness of the placing of cameras. So, we think CCTV should be looked at. The DNA database: we think there should be a presumption in favour of the removal of DNA from somebody who is not charged or convicted, a rebuttable presumption, but in some cases it may be necessary. I am thinking of something like Ian Huntley. It may be necessary to keep somebody's DNA even if they are not convicted, you know, if there are repeat allegations, but generally we think there should be a presumption for removal.

Q317 Chairman: Thank you. Could I just press the Parliamentary scrutiny point a bit. Dr Pounder, to some extent your evidence is slightly embarrassing for this Committee in the sense that it suggests the Home Office were able to put one over on us and on Parliament. We very clearly said there should not be a Citizens Information Project. You may have been given the impression there would not be one and you track how officialdom kept the Citizens Information Project going for months, if not years, and it then re-emerges as the core of the National Identity Register. Given that experience where, certainly when we were discussing the Identity Cards Bill, none of us knew that the officials were carrying on with this secret project, how can Parliament actually do the scrutiny role you want us to us do?
Dr Pounder: You invited me to say that that is why I recommended that this Committee should recommend removing section 1(4)(e) of the ID Card Act.

Q318 Chairman: Remind us, for any who may be watching on the Internet link, which section that was.
Dr Pounder: It is to do with the ability to share information, using the identity card database for a general public administration purpose. The other thing I would say is that this public administration purpose is subject to the review, it is called the Crosby Review, which is supposed to announce soon. I have given my evidence to the Crosby Reviewers with the hope, I have said to them, that if they are going to progress their ideas in identity management, it has to be through primary legislation and not through section 1(4)(e) of the Identity Card Act.

Q319 Chairman: Thank you. Ms Chakrabarti.
Ms Chakrabarti: I would agree with that. There are more general points about doing more in primary legislation. They do not just apply to privacy protection but to Parliament privacy scrutiny more generally and less by way of regulations after the event.

Q320 Chairman: Am I right in thinking, though, that the sort of Parliamentary role that you would like us as members of Parliament to play does require some quite profound reworkings of the way in which Parliament operates? You are fairly regular witnesses, all of you actually, to this Committee. You know the Select Committee's strengths, but also we are not full-time, we have many other commitments. How realistic is it to ask Parliament, as you actually see it, to play the sort of level of scrutiny role that clearly you all think in one way or another is the answer to some of these problems? I am not saying it is wrong, but it is a major change, is it not, to the way in which the Commons, in particular, works?
Ms Chakrabarti: Yes. There are general problems, but also there is a great opportunity at this moment to address some of them because we have a new Government and a new Prime Minister talking very much about trying to enliven Parliament. Privacy is a particular area, for the reasons we have discussed, that would benefit. I think you may at some point consider having a specific privacy committee just because the terrain is so considerable and the issues are not just constitutional, they are technological. So, with respect to your wonderful staff, you may consider some enhancement in your resource to do

that job. I personally, and Liberty, would like to see the Information Commissioner enhanced too, and we would like to see the Information Commissioner report to Parliament, be appointed by Parliament, and that could be true with some of the other public roles of that kind, but I think privacy in particular is such a qualified right, it requires such a constant public policy balancing act that Parliament really is going to be the court that enhances and defends it.

Q321 Mr Benyon: In relation to the point that Dr Metcalfe was making a moment ago about the wish that both your organisations want to have, transferring the power to intercept communications from the Home Secretary to the courts, you are quite happy to quote polling evidence that supported an argument that you made earlier. I suggest that the thousands of my constituents that use public transport in London, if they were polled on that, would say they would prefer it to stay with the Home Secretary because, if it went through a judicial process, it would be likely to take longer and, therefore, might put them at more risk, and at least they can get rid of the Home Secretary, if they feel he is failing, because he is elected. What do you say to that approach?
Dr Metcalfe: If there is specific criticism that prior judicial authorisation takes longer, it is worth pointing out that in Canada, Australia and the United States it is possible to get an emergency warrant without prior authorisation so long as the agency goes back to the court within 48 hours, sets out the reasons why they had to act as they did, given the nature of the emergency, and explains to the court what happened.
Ms Chakrabarti: It is not a full-blown criminal trial we are discussing here, it is just about who you trust to make this authorisation in a particular context, and we think one way to add to trust is to say a judge, not a High Court judge, perhaps something more akin to a magistrate—. It just seems appropriate that, where it can see such an intrusion with the individual, this is a particular role, this is something that a judge could do. There are many times in the context of anti-terror legislation where you and your colleagues say to the public a control order, or this, or that, or other measure would be enhanced by judicial involvement. Sometimes we at Liberty and JUSTICE agree with you, sometimes we do not think it kills the defect, but we do think that these issues of trust can partly be enhanced, not necessarily, as I say, by a very involved process, but by a judge, not a politician, issuing the warrant. We also argue in other contexts that there could be greater use made of Intercept product in criminal trials, and that is a debate that rages elsewhere, including in this Committee. So, if that were to happen, and that debate is being conducted, you are going to see greater transparency in any event.

Q322 Mr Benyon: Very quickly, you are saying you can have greater safeguards and a speedy process?
Ms Chakrabarti: Yes, you can.

Q323 Mr Benyon: As opposed to what we have at the moment?
Ms Chakrabarti: It is just about who constitutionally might be the better person to issue the warrant. When you search people's houses, as the police do and as they must do, because they have contraband or there is evidence of criminality, that is a warrant that is issued by a magistrate. Nobody finds that odd.
Dr Metcalfe: Courts make emergency orders all the time and late night injunctions. You have judges who are available 24 hours a day to grant injunctions or to make orders. It would be no different with intercept.
Dr Pounder: Can I add that you have the Home Secretary responsible for these organisations that interfere as well as the safeguards. This is an example of where you need to separate the two.
Chairman: Margaret Moran, last question.

Q324 Margaret Moran: This is to Dr Pounder. I think we have touched on the issues and you have referred to the data protection response being not up-to-date, increasingly disjointed, with the changes in government services being more joined up and, indeed, the technology. Some would argue, indeed some of the earlier witnesses and some of the research that has been done, that the greater problem is not so much increasingly disjointed data protection legislation as ignorance of what the data protection actually says. Can you comment what you would do in respect of the issue of disjointed data protection and the role of the Information Commissioner?
Dr Pounder: I did not catch the last part of the question?

Q325 Margaret Moran: What would your response be? What would you be looking to do in respect of what you see as increasingly disjointed data protection legislation, and if you wanted to comment on the role of the Information Commissioner in that context?
Dr Pounder: There are two elements. One of the problems, and why I think the Data Protection Act is in a sense weak, is that it is legislation that Parliament enacts because of the scrutiny element. For example, if you look at the data protection principles, there are many that use the word "purpose". So if you have a broad purpose, for example "efficient, effective delivery of public services", that actually negates the principle, so the Information Commissioner cannot do anything. What I would like to see from the Information Commissioner's perspective is the ability for him to exercise powers of audit, and I think the Commissioner has asked those. In relation to misuse of personal data, I think that the Commissioner should be able to have enforced, shall we say, powers of prosecution. One thing I would say on the transparency area: the Government knows that the European Commission has started, or begun, or threatened infraction proceedings that the Data

Protection Act is not a proper implementation of the Data Protection Directive and for two or three years all attempts to get to why the European Commission thinks the UK Data Protection Act is defective has basically come to nought. Of course, the Data Protection Act is central to what we are discussing today. One thing I would ask the Committee to do is to find out why the Government is refusing to publish the letter sent from the European Commission to the Department of Justice explaining why it thinks the UK Data Protection Act is deficient and the UK Government, for its part, to publish why it thinks the Data Protection Act is a proper implementation: because I think that would help sort out quite a lot of the problems of understanding how data protection relates to the 'surveillance society', as it is so-called.

Chairman: Thank you. That is a very helpful suggestion. Can I thank you very much indeed. I think it has been an extremely useful morning from both sets of witnesses, but particular thanks to the four of you.

Tuesday 20 November 2007

Keith Vaz, in the Chair

Ms Karen Buck
Mr James Clappison
Mrs Ann Cryer
David T C Davies
Mrs Janet Dean
Patrick Mercer
Margaret Moran
Gwyn Prosser
Bob Russell
Martin Salter
Mr David Winnick

Witnesses: **Mr Richard Jeavons**, Director, IT Service Implementation, Department of Health, **Mr Tim Wright**, Chief Information Officer, Department for Children, Schools and Families, **Dr Stephen Hickey**, Director General for the Safety, Service Delivery and Logistics Group, Department for Transport, and **Mr Steve Burton**, Deputy Director of Transport Policing & Enforcement, Transport for London, gave evidence.

Q326 Chairman: Mr Burton, Dr Hickey, Mr Jeavons, Mr Wright, thank you very much for coming to give evidence. This is obviously going to be a busy session and we have four witnesses from different Departments. What I thought would be helpful is if we could address our questions to each one of you. If there is a burning issue that you need to chip in on if you could do so quickly because I hope to end this session at about 12 o'clock. May I begin by asking Mr Jeavons the first question concerning the Department of Health taking the lead in government on these issues; what exactly does that mean?
Mr Jeavons: I think the Department has taken a very long and strong interest in the matter of confidentiality and the protection of patients' interests with regard to information, and necessarily so because without public confidence in how information about patients is managed we risk losing one of the fundamental tenets of how the NHS can operate. With the introduction of the National Programme for IT in 2002, clearly the need to examine further how information governance policy and practice is delivered in the NHS became even more important, and a steady stream of activity since then has strengthened our position. I think it is a combination of the fact that this is so important to the effective delivery of patient care and the introduction of the National Programme for IT means that we have had to seek to try and raise our game continuously over the last few years.

Q327 Chairman: What processes do you use in your Department to deal with breaches of security, in particular where errors have been found in records? How quickly are they corrected and how effectively do you deal with new processes in ensuring that those records are not defective?
Mr Jeavons: Most patient records are not held in the Department; they are held in the individual NHS organisations, and the responsibility for information governance rests firmly with individual NHS organisations as part of their statutory responsibilities. We provide guidance and policy on dealing with information governance and dealing with potential breaches. I can give you examples of where the NHS has acted to deal with breaches that have come to their attention, and usually (and having a run an NHS organisation myself I can testify to this) this follows a formal disciplinary process because it inevitably involves individual members of staff.

Q328 Chairman: How will the National Information Governance Board go about adopting and maintaining high standards?
Mr Jeavons: The National Information Governance Board came into being on 1 October. We are hoping through the Health Bill to give it a statutory basis. This will effectively require every NHS organisation under its remit to provide an annual report on its information governance, it will review policy and practice and make recommendations on improving them, and it will report its findings to the Secretary of State on an annual basis, so it is an extremely high-level and visible statement of the accountability for information governance and it is directly connected both to policy and into practice in the NHS.
Chairman: Ann Cryer?

Q329 Mrs Cryer: Richard, could you tell us what strategies the Department of Health will be using to ensure that patients are able to make informed choices about how their information is held and stored?
Mr Jeavons: Yes. The responsibility for ensuring that patients are reasonably well-informed exists already. It pre-existed the National Programme for IT. The route we have gone down is to reinforce and to clarify the responsibilities of individual organisations. If I give you a specific example, in last year's Operating Framework, which is the annual statement of what the NHS should do in its plans in the coming year, we gave an absolutely explicitly steer to NHS organisations about reviewing their information governance position and being able to answer simple questions that patients might ask them should they be approached. That would be an example of how we are really trying to make a very high-profile but very practical focus at the top of organisations for their responsibilities. Another example is public information programmes. We encourage and support the NHS when they are considering changing the use of information to improve patient care to run public information programmes to ensure that their population has the opportunity to engage in a discussion. For example,

the Summary Care Record early adopter programmes in Bolton and Bury would be examples of what we are doing, and we are evaluating those. You can always do these things better: you can learn from Scotland, you can learn from Hampshire, you can learn from places that have done things, so it is a continuous process. We have methods that we are trying and evaluating and we are encouraging the NHS to do that as well.

Q330 Mrs Cryer: Just to dig a bit further, can you tell us what sort of support and help will be available to clinicians as they give advice on patient choice and consent?
Mr Jeavons: To go into the Summary Care Record early adopters, which is the most vibrant and real example at the moment, we are running a public information programme which involves a personalised letter to every person over 16. Those are backed up with access to an NHS Direct helpline. When people phone in, the staff in NHS Direct have been trained and given tools to help them answer the questions effectively. We are running information booths where patients can book to meet people in their practices and health centres. The staff who are providing the advice there are trained and we have provided an e-portal of training materials for general practitioners to use as well. To be fair, we are not at the stage where a lot of general practitioners are directly engaged with their patients in these discussions but that is coming in the next few months.

Q331 Mrs Cryer: Therefore how will the Department of Health, just to take it further, interact with the National Information Governance Board as it seeks to "be ever watchful and in touch with public perceptions"?
Mr Jeavons: The National Information Governance Board will produce an annual report to the Secretary of State. It will have a statutory basis. It will seek advice and accept views from anybody who wishes to approach it, so it will operate in a very open way. When it thinks it has got a set of questions it will seek, directly from the Department of Health's Information Governance Policy and related advice, to answer the questions and try to reach conclusions. In a sense, we have aligned the information governance capability and advice and policy support behind the Information Governance Board's roles and responsibilities, but it has to retain a strong element of independence.

Q332 Mrs Cryer: So if I can just be informed and ask; whilst witnesses in our inquiry spoke of the use of patient information for research purposes as an example of one of the benefits of "surveillance", they also identified "a climate of suspicion" around the use of patient information for research purposes. Therefore what steps is the Department of Health taking to tackle concerns about the security of information used in this way?
Mr Jeavons: Most recently we have had two quite major joint pieces of work which are now guiding what we are doing. Those pieces of work are the Joint Report with the UKCRC that was commissioned, which Ian Diamond led for us, and the recommendations of that were accepted, and the Boyd Report, which was commissioned by the predecessor of the National Information Governance Board, and again the recommendations were accepted. Those two reports made a number of recommendations about what needed to be done to bring greater clarity, to reduce ambiguity, and to sustain and develop confidence in the area you are asking the questions about. In response to that, we have established a research capability programme which has a work plan to work through those recommendations. Anonymisation and pseudonymisation techniques were raised as issues and we are reviewing those. We have looked at the current use and we have done an audit of the current use of some of the information in order to test whether we think the current practice is fit for purpose and is being sustained. We have a number of activities over the next 12 months which are aimed to respond and deal with those recommendations.

Q333 Mrs Cryer: Just to dig a bit further and to refer to another select committee, the Health Select Committee apparently did a recent report on the Electronic Patient Record which registered concern about governance arrangements for the use of patient information for research purposes. The Secondary Uses Working Group has made recommendations on this aspect of the development of NHS care records. Are you able to give an indication of how the Department is taking these recommendations forward?
Mr Jeavons: I think those recommendations are in the Boyd Report that I have referred to, and the National Information Governance Board have already agreed that they will ask the Department to demonstrate that they have delivered against those recommendations and those recommendations are being actioned through the research capability programme.
Mrs Cryer: Right, thank you.

Q334 Margaret Moran: It sounds as if it is all going terribly well when we know it is not. Just look at *Computer Weekly's* history on this subject and you can tell that is not the case. I have two questions. One of the issues around data-sharing is that even if you get the technology right, the problem is access by people and the use or misuse of data in that way. Given that there was not apparently a buy-in from front-line staff and there was not even proper consultation of front-line staff at the outset of this programme, how confident are you that there will not be breaches of data and confidentiality and privacy as a result of that?
Mr Jeavons: You cannot stop the wicked doing wicked things with information and patient data, so you cannot say there will not be, and of course we have examples where staff do misuse their privileges and have to be pursued through disciplinary and other procedures. To speak to your point about confidence, there is absolutely no complacency about the extremely fine balance that we need to

strike between public confidence, staff confidence and the huge potential benefits that electronic records and the use of data about patients for public health and other purposes has. This is an incredibly difficult balancing act and practice needs to change as information technology changes the opportunities that are available to us. The reinforcement with the NHS of their information governance responsibilities; the backing up of that with advice and tools; the reinforcement of the need to ensure that human resources policy and practice is aligned with information governance policy and practice means that we are putting in place all the things we can do to deal and to manage this as well as possible, but we are not going to stop those who wish to break their employment contract terms and break their local Human Resources policies and procedures and do wicked things. What we have to do is put in audit trails and be able to say to these people it is much more likely now that you are going to be caught, and if you are caught this is how you will be dealt with.

Q335 David Davies: Mr Jeavons, what work have you undertaken with other government departments in relation to the sharing of databases? In particular, can I ask you whether you work with the Border and Immigration Agency or the Department for Work and Pensions, to ensure that non-EU citizens do not access incorrectly out-patient care to which they are not entitled?
Mr Jeavons: Our main areas of interaction are with the Department for Children, Schools and Families and with Contact Point. We contribute and participate in cross-government policy and Transformational Government activity. We respond to requests for information that have a legal basis. However, our basic opening position is that NHS information and information about patients is confidential to the NHS and to the patient and therefore we work on a "persuade us if you can or provide a legal basis" mandate.

Q336 David Davies: But would you not use the databases that are already available to other government departments to ascertain whether or not people are getting access to care to which they are not entitled?
Mr Jeavons: I am not aware that it is the case that we do that and it is not clear that that is necessary. We do not deny emergency care.

Q337 David Davies: No, we would not do that under the law anyway, would we, because the law is quite clear; emergency care is available but out-patient care is not. The question is purely about out-patient care and whether you are doing anything to tackle the billions of pounds that are being lost because out-patient care is being provided to people who are not entitled to it?
Mr Jeavons: Clearly if we had evidence that there were billions of pounds being lost through inappropriate use of NHS services that would need to be tackled. If the opportunity were there for example to use other means to check the identity of people before they access those services, then those would be looked at, but I am not aware that those opportunities are there and, if they are there, it is not obvious how to implement them effectively in the NHS at the moment.
David Davies: The evidence is certainly there, is it not; the question is whether or not the NHS are willing to make use of other databases that already exist in government departments, but I think you have answered the questions.
Chairman: Thank you, Mr Davies. We are now turning to questions to Tim Wright. You are welcome to sit there, Mr Jeavons, because there may be other issues that members of the Committee will ask, so do not feel we are ignoring you. It is just we want to get the other Departments to give us their comments as well. Janet Dean has the first question to Tim Wright.

Q338 Mrs Dean: Mr Wright, could you estimate the proportion of DCFS activity that depends on information-sharing and the impact that the Every Child Matters strategy has had in this respect? In doing so, could you say whether the majority of activity is aimed at child protection or child welfare?
Mr Wright: A very significant part of the activity of the Department now is geared around data-sharing. We are quite a small central department operating within a very large, very profuse education sector, so there are many agencies and bodies that operate within that sector who will need and wish to use and share information. A number of the programmes that we are working on at the moment operate in that sphere and are quite central and quite key to supporting the Government's policy to improve choice for learners and enable individuals to move round, if you like, within the education system and take with them their personal records and details and be able to track their attainment and so on. On the second part of your question—my colleague here already mentioned Contact Point and of course I would draw a distinction between the purpose of Contact Point, which is really early intervention to ensure the protection of young children, with the sorts of systems that we are operating, which are purely in the educational space which are trying to engage with people in education. There is quite a split and quite a wide range of activities that are there. I would not hazard to put percentages on that because there is a very significant effort from the Department, certainly around Contact Point, and that is the largest single IT programme that we have on at this time.

Q339 Mrs Dean: I will come to Contact Point in a minute but could you say first of all how the Department goes about assessing the need for each new database that it creates or commissions and then drawing up the protocols for sharing information with other departments or agencies?
Mr Wright: I look after a team of information technology professionals and certainly we work extremely closely with the policy directorates of the Department to understand how technology might be applied to improve the opportunities for learners

and children. It is quite a tight engagement, quite a tight partnership, between the technical professionals that provide and support the information systems and the infrastructure, with those that are actually in the front-line of delivering the Government's policy. There was a second part to your question, I am sorry?

Q340 Mrs Dean: It was about drawing up the protocols for sharing the information with other departments or agencies.
Mr Wright: I am not aware of any outward sharing, if you like, of information from the DCFS. We certainly rely upon other government departments to provide information to us. Contact Point again would be the best example of that where in fact we take national data feeds from three other Departments—the Department of Health, the Department for Work and Pensions and the Office for National Statistics—and we combine that in Contact Point with data from our own records from the pupil database.

Q341 Mrs Dean: To turn to Contact Point, the Assistant Information Commissioner describes how the ambitions behind the database which is now Contact Base "started out as rather greater and have fallen backwards a little bit". Could you summarise the history of the Contact Point database in terms of the development of its objectives and scope?
Mr Wright: I am not actually familiar with its long history. Clearly the history of the database goes back to 2001 and the Victoria Climbié case, but in the time that I have been engaged with Contact Point, the mission for the Department around Contact Point has not changed in any way. The system is an electronic index of every child in the country, with the sole purpose of bringing together those care professionals that work with children and need to be aware of other care professionals within the system that may be working with the same children.

Q342 Mrs Dean: So you do not really agree with the Assistant Information Commissioner that there has been a pull-back from the ambitions that were once there?
Mr Wright: I am not aware that there has been a pull-back. I have been with the Department for most of this year, I was not in the Department at that time, but I am not conscious that there has been any watering down or changing of the Department's ambitions for Contact Point.

Q343 Mrs Dean: It may be something that you could look into for us?
Mr Wright: I would be glad to.

Q344 Mrs Dean: In designing Contact Point do you know what steps have been taken to ensure that the information collected about children is accurate and that the positive outcome in terms of child welfare outweighs any loss of privacy so early in life?
Mr Wright: Yes, the basic data on which the system relies is taken from four other data sources. What the system actually does is bring those four data sources together and then matches the data sets. There is a significant amount of overlap in those data sources so you will be picking up children's names, home addresses, and so on from all those different data sources. What we do is use the technology to match those databases and prove by overlay, if you like, that the data is indeed correct for each of those children. There are exception reports which are produced on a routine and regular basis to highlight anomalies that may require further investigation.

Q345 Mrs Dean: Which are the four data sources?
Mr Wright: They are taken from the Department of Health, from the benefits system of the DWP, from the birth registers of the Office for National Statistics, and from our own national pupil database.

Q346 Ms Buck. I was surprised to hear you list the three Departments and not include the DCLG. I just wonder if you could tell us a little bit about the relationship the Department has in respect of information from local authorities, in particular from all the sources in the DCLG?
Mr Wright: We do have contact with the DCLG in relation to Contact Point but not in regard to data-sharing. Our particular contact with the DCLG is to ensure that the infrastructure over which Contact Point is delivered is going to be delivered in a way which will enable local authorities to most readily and easily use the system in a secure way. There is no output flow of data to DCLG and there is no data actually coming from them. The infrastructure of the system is actually something that from local authorities' point of view is extremely important because of course now and into the future the expectation is that they will wish to access a number of systems from different departments. We are very keen to ensure that the mechanisms by which they access those systems are compatible and it is not a burden put upon the local authorities to connect to lots of different systems.

Q347 Ms Buck: In terms of the local authority Every Child Matters agenda your involvement in this is purely an infrastructure and data compatibility one?
Mr Wright: Certainly from my own group's perspective but, no, a very significant part of the Contact Point programme is actually working closely with the local authorities to make sure that there is robust education about what the system can do, how it should be used, how it should be protected, and the security that is in place and so on, so there is certainly a very active dialogue with the local authorities to ensure that the system will be effective in its use.

Q348 Ms Buck: How do you see local authorities' various sources of information currently within the Every Child Matters framework fitting into this? To give you an example that goes to the heart of it for me, and it goes to the heart of a lot of the data protection issue—the NOTIFY system for children in temporary accommodation because this is very

much about children who drop through the net—I am not quite clear of the importance that local authorities should be putting on systems like that, which go very much to the heart of children at risk and child protection, and how they will fit into a national Every Child Matters data framework as you are describing it.

Mr Wright: Contact Point, as you rightly describe, is a national system to be accessed and used by every local authority. Each local authority in the country will also have a number of its own support systems and case management systems that do actually hold detailed information about particular child cases. What is important to us is to ensure that we are delivering the infrastructure of Contact Point in a manner in which it can be integrated at the local authority level with their local data sources to present a full picture, but of course the case information that local authorities hold is solely for their purposes.

Q349 Ms Buck: So none of that will be uplifted into—

Mr Wright: No, no lift goes upwards but we need to be able to connect systems at the local level.

Q350 Ms Buck: Can I just ask you about the potential of developing biometric data in education and schools. Where has that got to, where is the thinking and does the Department expect there to be a time in the near future when children will be expected to carry some form of biometric recognition?

Mr Wright: Surely. Biometric systems are used within a number of schools within the UK. There is no drive from the DCSF to promote the use of biometric systems but we are very conscious of the fact that a number of schools find them quite beneficial. They are used in schools for the purposes of monitoring attendance, of providing children with facilities to remove library books or to purchase school meals. There are a number of benefits of using biometric-based systems over other technologies such as smartcards, principally the fact that the child does not have to carry anything with them and therefore do not lay themselves open to bullying tactics from other children that may wish to get hold of their card in order to access the services that they have.

Q351 Ms Buck: Do you think that we should be comfortable with the idea of biometric recognition for getting out a library book?

Mr Wright: Certainly the Department is quite content with the use of biometrics in that way by school children. It is a very effective mechanism. Biometric data that is held by these systems is of quite a low quality in the sense that it is only held at a level which will enable a school to differentiate amongst the school community, so there is no value in that biometric information outside of the school environment.

Chairman: Thank you, Karen Buck. Margaret Moran?

Q352 Margaret Moran: Given your technological capacity and capability and the fact that you are dealing with a number of children's databases, how much further do you think there will be progress or otherwise in relation to further data-sharing and data-gathering? Is there greater scope for any of that?

Mr Wright: I think over the next few years we are certainly going to see significant progress around the initiatives that we have already started. I mentioned when I started about being able to join up this very large and quite complex education system that we have in the UK, so it is about improving choice for learners. Our expectation is that there will be a number of other future participants in the initiatives that we have already started. We have a programme we call MIAP (Managing Information Across Partners) which is very specifically to support the Government's drive for reforming the 14 to 19 age group. MIAP actually underpins the diploma environment and it is going to be very important that children can take their information from one institution to another and can have their qualifications recognised on their lifetime journey. I do not see on the horizon any particularly new initiatives at this time. I think it is quite inevitable that we will find that we will wish to continue to provide that kind of shared information infrastructure across the education system. I do draw a distinction perhaps between education and the care and welfare of children, and when it comes to systems like Contact Point there is very clear regulation in place for systems such as Contact Point, so I see no drift from that. Contact Point is there for a very specific purpose and that is the backstop to what that system will be used for.

Q353 Margaret Moran: I want to come back to Contact Point later. You are talking about data-sharing from pre-school nursery through to 19, to the end of HE, something like that?

Mr Wright: Well, in fact in information terms I am talking about what we would refer to as the lifetime journey of the learner, so I am talking about, yes, from the early years right through to adult and workplace training. In the changes in government this year the Department for Education and Skills was split to create the Department for Children, Schools and Families and the Department for Innovation, Universities and Skills. In terms of lifetime information-sharing that effectively cleaved a line at aged 19 in that learning journey, but with colleagues in the DIUS we see a very strong need to continue that co-operation between the two Departments to ensure that the education system in the country remains joined up.

Q354 Margaret Moran: It is very expensive data-sharing based on very different systems very often. How can you ensure inter-operability and ensure that there is no rubbish-in rubbish-out? Where do you think the technology will take us next? Are we looking at data-mining, profiling, prevention?

Mr Wright: Sorry, can you just repeat the first part of your question.

Q355 Margaret Moran: I have forgotten it myself! Where do we go next in terms of technology and interoperability?
Mr Wright: Thank you, I think the key word was "interoperability". Joining up across government is extremely important in lots of different areas. I have a role within the Department for Children, Schools and Families to support the policy directorates in managing information, but I also have another role as a member of the information community across government, so we have mechanisms at a higher level, if you like. We have a CIO Council that comprises members from all government departments, and a very significant part of our agenda and our thrust through the CIO Council is to ensure that we have a common framework for data standards and can share best practice across government departments, so in areas such as data security, for instance, those thrusts to ensure that we have the right levels of security in place and we are using technologies that are available as wisely as possible is the sort of thing that is done at a higher level, if you like, through the CIO Council, and that is quite an active community.

Q356 Margaret Moran: Just very quickly on Contact Point, you will be aware, more than anyone I guess, that there are serious concerns about the amount of data being collected on children and whether lack of confidence in the ability to keep that data confidential will deter people from accessing the services and indeed possibilities that having all that data together could actually put children at greater risk. What research has your Department done to ensure the effectiveness of communication about what is actually happening on data-gathering and data-sharing in that context?
Mr Wright: I would describe Contact Point itself as an electronic index. It is true that it will include data on every child in the country but it is only basic demographic information, so it is child's name, date of birth, address, parents' names, the learning setting/the educational setting in which they are currently residing, GP's name, and other specialists that they may have contact with. There is no case information within Contact Point whatsoever. Whilst the Contact Point programme is a significant technological challenge, we recognise that communication across the community of users of Contact Point, of which there are many thousands, is a crucial part of the success of the system, and that is a very active dialogue with that community. As part of the first phase of the use of Contact Point, which will commence during next year, we will be working, and have started working very closely, with 17 early adopter local authorities so that we can work closely with them and learn the lessons of early adoption and make sure that that knowledge and that practice, if you like, is shared and cascaded to other users of the system.
Chairman: Thank you very much, Margaret Moran. We are now turning to some questions to Dr Stephen Hickey from the Department of Transport and we are going to start with Martin Salter.

Q357 Martin Salter: Dr Hickey, I was interested in your memorandum of evidence to the Committee and in particular in paragraph 4 where you talked about clarity about the legal authority under which data may be shared, including using the Data Protection Act, being critical. I want to tease out a couple of examples. Has your Department had any requests for data from other government departments or other areas of government which you have considered not to be lawful?
Dr Hickey: I cannot think of one offhand where we have specifically rejected it on that ground, but we certainly do review the legal basis on which we do data-sharing. Most of our data-sharing is fairly long-standing but we would certainly want to know on what basis any approach was made to us and what was the legal justification.

Q358 Martin Salter: Because at the moment the way the process works is that government departments and other agencies seek advice from the data protection authorities and also from the Information Commissioner and it is possible that cracks could open up and people could end up with different advice and different practices could emerge.
Dr Hickey: But we would need to look at it from both ends of the telescope. We need to look at it both from have they got the power to seek the information but also have we got the power to give it, so we will ask both those questions.

Q359 Martin Salter: One final question from me. I notice in paragraph 2(7) of your evidence there is perhaps a more contentious area than a government department, which is the sharing of data with parking enforcement companies. It says here that you will do this where they can show reasonable cause to receive the data. Of course some parking enforcement companies are nothing more than licensed thugs to clamp vehicles in dubious circumstances. Do some of the clamping—I will not even call them organisations—outfits benefit from data provided by your Department?
Dr Hickey: There was a big review of this done last year and ministers announced 14 improvements to the processes around reasonable cause. Reasonable cause are the words used in legislation but there is not a definition in law. 14 measures were announced last year to tighten up on the processes around reasonable cause and who should get the information. Amongst those is a lot more transparency around the information which is now, for example, on the DVLA website and on Directgov, so there is a lot more visibility to people on the circumstances in which information can be provided. As far as parking companies are concerned, there are two set of processes, one is for ad hoc individual requests, and the companies have to go through a process to justify why that is needed and they are asked various questions about their business and the purposes and so on, and that can be checked and audited, and refused of course if those answers are not acceptable. In addition, for companies who are doing it on a regular basis, which of course some of them are, and where we have

electronic links, they are required to register with us, and they go through processes of validation including of their internal processes and they are also asked to be members of an approved association which itself has various processes for control. All of that is much more transparent now than it was two years ago. As I say, a lot of this is now on the website and our feeling is that the processes are now working more satisfactorily than when this issue was raised quite strongly a couple of years ago.

Q360 Mr Winnick: Dr Hickey, there are a lot of cameras all around the place operated via the Highways Agency. In the very useful paper that you circulated you give at paragraph 1.4 details. Apparently there are 1,133 automated number plate recognition cameras and 1,300 CCTV cameras. How far are motorists in the position to be able to check on the website who is actually responsible for those cameras?
Dr Hickey: I think those cameras are the responsibility of the Highways Agency, but of course the Police have many other cameras and there are many other people—local authorities and others—who have cameras. I think those ones you referred to are all Highways Agency cameras.

Q361 Mr Winnick: How far would motorists be in a position to contact the Agency because presumably in some circumstances they may wish to do so?
Dr Hickey: They can certainly contact the Agency. I do not know offhand whether on the website it would tell you where each camera was. I suspect not, partly because of course some of them are moved and are mobile.

Q362 Mr Winnick: I will come to criminality, which is the purpose of these cameras, they are not there for fun and no doubt they serve a positive reason. However, would it not be useful for the ordinary citizen to be able to find out from the website precisely what is what?
Dr Hickey: Yes, I accept that point.

Q363 Mr Winnick: Is it intended to have more sophisticated technology in time? It is not the end, is it, these cameras which I have mentioned a number of which are in use? Are they going to increase? Are there going to be other different kinds of cameras?
Dr Hickey: The need for cameras certainly has been going up. For example, if we go further down the route of active traffic management on the network, the sort of system with traffic controls that we now see on the M42 around Birmingham where you have got hard shoulder running for example at peak hours and tighter speed controls and a need to watch extremely carefully if incidents were to happen, then clearly that sort of operational system relies quite heavily on these cameras. If we go further down the route of that kind of regime on the trunk roads, then certainly the need for active management, including cameras, is likely to increase.

Q364 Mr Winnick: Just tell us, Mr Hickey, how long has this been happening with the cameras? How many years back? Presumably there was a time, including in the post-War period when people would drive without cameras and investigations and so on and so forth?
Dr Hickey: I can tell you from personal recollection that in the 1960s cameras were introduced in Durham City for the control of traffic coming up from the bridges to the market-place because I was a boy at the time and it was a very big deal and we used to go and stand behind the policeman's box and look over his shoulder at these cameras, it was a major novelty, and Durham prided itself on being one of the first towns to have that sort of camera. That was the 1960s, I think. On the national network I am afraid I do not know offhand when they started.

Q365 Mr Winnick: We are talking about 40 years.
Dr Hickey: Cameras have been around certainly to my personal knowledge—

Q366 Mr Winnick: And all the indications are that it is escalating, is it not?
Dr Hickey: On the roads but also more widely in local authority communities and so on cameras have certainly increased substantially.

Q367 Mr Winnick: I said a moment ago—and I do not think there is any disagreement—that they are not there for fun; they are to deal with those who break the law and outright criminality, but what I want to ask you is, how do you assess the potential benefits for example of these number plate recognition cameras which I have mentioned compared with the risk of mistakes or criminal misuse—that is going further—of transport databases?
Dr Hickey: Could I first just correct you on the Highways Agency cameras. The Highways Agency cameras are not used for criminality in quite the sense I think you are implying. They are actually used for traffic flow control. That is quite important. For example, they do not record the full number plate of the individual vehicle, which of course for criminal-type purposes you need to have. The Highways Agency ANPR cameras only record three digits, which is enough to say at the next point down the road those same three digits can be identified and from that you can calculate what the flow of traffic is. That is not enough to tell you it was my car or someone else's car.[1]

[1] *Note by witness*: Highways Agency ANPR cameras are used for traffic management purposes and do not record the full number plate of the vehicle. However, this is not achieved by recording only three digits of the plate. The actual process is that, at the point of capture, the registration number is encrypted into a permanent non-reversible string of text. The outcome though is the same, ie vehicles passing the ANPR camera sites cannot be accurately identified or cross-referenced against other databases. But it is by the encryption mechanism rather than by dropping characters from the registration number.

Q368 Mr Winnick: So it would not help the Police?
Dr Hickey: It would not help the Police, no.

Q369 Mr Winnick: What would help the Police in carrying out their investigations?
Dr Hickey: For the Police's purposes you need the full number plate and of course the Police do have ANPR cameras that show the full number plate. They are both ANPR cameras but they are used in different ways and for some different purposes, and we must be clear.

Q370 Mr Winnick: So the motorist—and I am not saying that should not be so, we recognise all the criminality that could be involved—on all these roads is constantly being watched?
Dr Hickey: That is right. As far as criminality and so on is concerned, the ANPR cameras, which are particularly relevant to that are the Police's own ANPR cameras and they have a lot of those, as you know. In addition, from the Department's point of view, as you will have seen from the memorandum, both DVLA and VOSA have a small number of ANPR cameras, nothing like the Police scale. Those are used for identifying vehicles which are not taxed or, in the case of VOSA, have other HGV concerns about them, so those do identify the individual vehicle.

Q371 Mr Winnick: That is a very useful answer. In terms of our inquiry we would be right presumably to say that the use of cameras and such technology is likely to increase rather than decrease?
Dr Hickey: I think that is plausible.

Q372 Mr Winnick: More than plausible?
Dr Hickey: Yes.
Chairman: I shall bring Mr Davies in now for a quick supplementary.

Q373 David Davies: Just to turn around one of Mr Winnick's questions, the whole point of ANPR readers is that they can track a licence plate registered to a criminal and find out where on the motorway for example that person is exiting so the Police can follow that up. Would it be useful to advertise to the whole world where ANPR cameras are located or would it not defeat the whole purpose, which is to be able to track people who should not be on the road?
Dr Hickey: You are quite right that for Police cameras which do that sort of thing certainly it would be quite counter-productive to tell people but for traffic monitoring purposes there is not that same sensitivity, so it is a more open question.

Q374 Chairman: Could I ask you to comment on the new proposals that passengers on domestic flights between Northern Ireland and the UK mainland are now to be subject to identity checks; is that coming from your Department or the Home Office?
Dr Hickey: I confess that is not a subject I am familiar with. I can come back to you and tell you which department is behind that.

Q375 Chairman: I think it is a Home Office Statutory Instrument but obviously the Department for Transport would need to have been consulted.
Dr Hickey: That is probably right, yes.

Q376 Chairman: Would you drop us a note on that?
Dr Hickey: I will drop you a note.
Chairman: Thank you so much. Patrick Mercer now has the first question to Mr Burton for Transport for London.

Q377 Patrick Mercer: Has Transport for London itself commissioned any research into the effectiveness of CCTV as a deterrent to crime on the transport network?
Mr Burton: We have not undertaken any specific research on that. We have done a fair amount of research on passengers' views of CCTV.

Q378 Patrick Mercer: Who are very reassured by it, are they not?
Mr Burton: Indeed, all our research, as you say, shows that passengers see two primary ways of making them feel safe on the network: visible, uniformed staff; and CCTV systems.

Q379 Patrick Mercer: Okay, but you have not actually taken any soundings yourself as such?
Mr Burton: We have not got any empirical research on the actual results. We have results-based analysis done in specific areas, for example the on-bus CCTV systems that we use which are primarily there for crime and disorder reduction, we have had some very positive results around that where we have identified over 2,000 individuals and convicted 2,000 individuals who have been damaging and vandalising the network. In certain areas we think we have got good results but because a lot of the systems are recently installed we have not actually undertaken any detailed research of the overall systems.

Q380 Patrick Mercer: After a crime has been committed and the Police want evidence from your camera systems, how do they go about retrieving data from TfL sources?
Mr Burton: I have a small group of individuals working for me. The Police fill in the appropriate data protection form to identify why they want the data and we will do our best to give them the appropriate information. We do that in a transparent way and we have fairly carefully structured guidelines for those staff on when it is appropriate to release the information.

Q381 Patrick Mercer: I appreciate there may not be an exact answer to this but on average how long does that process take?
Mr Burton: It will take a couple of days at most. Essentially we work with the Police very closely and we will prioritise cases. Obviously the more serious the case the more resources we will put on it, and we will do our best to turn it around in an appropriate timescale.

Q382 Patrick Mercer: You will be aware that there is a debate going on about whether the public should or should not in certain circumstances have access to the data that you have gathered. What is your view on that? If a crime has been committed and the public needs to have access to your data, how far has the debate gone?
Mr Burton: Obviously there is a debate going on around that. There are currently a number of FOI applications that people have put in and we will treat them on a case-by-case basis. At the moment we have no plans to make that data available as a matter of course and I think we would want to work very closely with the Police agencies on that. By their very nature most of those requests that come from the Police are active investigations so there are sub judice issues of course as well.

Q383 Patrick Mercer: Can you give me a feel for what the volume of those requests is?
Mr Burton: At the moment we get just over 300-350 requests for specific pieces of data, on the Oyster system for example.

Q384 Patrick Mercer: How often?
Mr Burton: Per month. However you have to contextualise that. We are running three and a half billion journeys a year, so in comparative terms it is a fairly small number.

Q385 Ms Buck: Can I ask you a bit more about the gauging of public opinion because clearly there is out there some degree of concern about surveillance of customers and users of all kinds of services. Do you have any sense at all of the extent to which users worry about their privacy and how would you research it?
Mr Burton: We have done a number of market research exercises of both customers and the community at large because they are two different groups in many ways. A particular exercise we did a year or two ago was asking people what we could do to the network to make them feel safer. As I say, I think the second item that was identified was putting more CCTV on to the system. We do consult on a regular basis on how we use the system.

Q386 Ms Buck: But do you ever ask them the flip-side question, the extent to which people feel that even making a simple journey now puts them under surveillance? Is that angle of it addressed by anything that you research?
Mr Burton: We have not asked them recently on that. There is a piece of research we are doing at the moment for which I do not have the results available, in fact it has only just been done. Our information access team, who run our overall data protection work, have asked members of the public how they feel about accessing our data and how they feel about being observed. I think those results will be out in the next few months, but the previous stuff we have done, as I say, does show that the public do feel comforted by a feeling of being watched on the network. I think it might be different if you ask people outside of what they perceive to be a controlled environment, but I think the public very much see the public transit system as something we should manage on their behalf.
Ms Buck: Of course they do but if you do not ask them you are not going to know where that balance is struck. Perhaps we could ask for the results of that survey to be shared with us.

Q387 Chairman: That would be very helpful. Could you send that to us?
Mr Burton: We will do.
Chairman: Thank you very much. Mr Davies has a question on the Oyster scheme. I should declare I have an Oyster card.
Ms Buck: So do I.
David Davies: I think my question was probably answered by something that the gentleman said. It was to do with the number of requests that the Police had, so I am content.

Q388 Chairman: Before I release you all, I have a question on the practical measures adopted by my local health authority. When a constituent comes to me and asks about the length of time it takes for him to get an operation, for example he wants an earlier date, I would write to my local health authority and expect to get the information back. They have now adopted the practice of writing back to me and sending a consent form for me to send to my constituent in my constituency to sign and for it to be returned to me and then returned to the health authority. Do you know what the practice is with different local health authorities because I would have thought it was implicit that when a constituent walks in and sees a Member of Parliament that they have given consent for the MP to write.
Mr Jeavons: The answer is I do not know what the practice is across local NHS organisations. I am quite happy to look into that though and provide a note.
Chairman: I do not know what other Members have found.
David Davies: It is good question.
Bob Russell: It sounds like a Leicester problem. It does not affect me.

Q389 Chairman: I think we are all nodding in agreement and chuntering and saying this happens to us, too, so if you could find out that would be very helpful. It may be an attempt to delay matters so that the operation takes place before the answer is given, but who knows.
Mr Jeavons: I could not comment.
Chairman: Mr Jeavons, Dr Hickey, Mr Wright and Mr Burton, thank you very much for your evidence today.

Witnesses: **Ms Clare Moriarty**, Constitution Director, Ministry of Justice, and **Mr John Suffolk**, Her Majesty's Government Chief Information Officer, gave evidence.

Q390 Chairman: We now welcome to the dais Clare Moriarty from the Ministry of Justice and Mr Suffolk who is the Government Chief Information Officer. Thank you for coming to give evidence to us today. If I could start with you, Ms Moriarty, the Ministry of Justice we are told "holds the ring" across government in terms of data protection and data-sharing. How does this work in practice as far as day-to-day issues are concerned?
Ms Moriarty: The Constitution Directorate within the Ministry of Justice is responsible for rights and democracy issues, and as part of that we lead the Government's domestic, European and international policy on data protection and data-sharing, and as part of that we are responsible for the operation of the Data Protection Act. As the volume of data that is collected and shared increases that obviously creates opportunities for crime prevention, for tackling social disadvantage and for improving public services. What we have to do is to ensure that as we exploit those opportunities that they are balanced against the need to protect people's privacy. The responsibility for privacy aspects of individual policies rests with the departments responsible, as obviously you have seen in the evidence you have already had today. Our responsibility as the Ministry of Justice is to work with departments to ensure that they remain compliant.

Q391 Chairman: So you advise them?
Ms Moriarty: We advise them.

Q392 Chairman: And on a European level you take the lead?
Ms Moriarty: On a European level, if they are individual policies, they will take the lead. We lead on negotiating general instruments.

Q393 Chairman: And then you will come back and give advice to other government departments?
Ms Moriarty: Yes, and particularly on European and international issues we have created a group of interested departments and we work with them on data protection and data-sharing issues.

Q394 Chairman: Do you act as arbiter between departments if one department is keen to get information from another and they do not want to give that information? Would you step in and advise?
Ms Moriarty: What we would do is work it through with the departments. The critical issues to be looked at are: is there a purpose for sharing information; do the powers exist to share the information; is any intrusion on privacy proportionate to the benefits that will be gained from sharing the data; and is the data going to be adequately protected in terms of the principles underlying the Data Protection Act? Essentially that is a set of issues to be worked through. Where there is more than one department involved we would help them work through those issues so that they reach an agreement.

Q395 David Davies: One specific question on this—and I have been trying to find out the information for some time without much success—and that is whether or not the Department for Work and Pensions accesses databases used by the Ministry of Justice effectively in order to find out whether people claiming benefits are actually on the run from open prisons. You might think it is so glaringly obvious whether that can happen and yet when I have written to the Ministry of Justice, or its previous incarnations, I have not been able to get a clear response. Do the Department for Work and Pensions check a database, presumably in the Prison Service, of those who have walked out of open prisons to ensure that they are not accessing benefits? There are thousands of people on the run and they are not all living in the woods eating squirrels and wild berries.
Ms Moriarty: The straightforward answer to that is I do not know. The individual arrangements that the Ministry of Justice makes would be owned by individual parts of the Ministry of Justice. If you would like me to take that away and try and find an answer—

Q396 David Davies: Would you? That would be great. You will have more success than I have had.
Ms Moriarty: Hopefully.

Q397 Chairman: I think, Ms Moriarty, that you just have to go next door, do you not, somewhere in Selborne House the answer must be there?
Ms Moriarty: Somewhere in Selborne House the answer certainly should be.

Q398 Bob Russell: Mr Suffolk, two relatively brief questions. I understand that part of your role involves enabling "public service transformation through the strategic deployment of technology". What do you see as the most significant developments in technology from the point of view of delivering public services? Linked with that, how do you fulfil this role across government, if at all?
Mr Suffolk: The first part of the question first. Without a shadow of a doubt I think technology is moving at its fastest rate ever, it is accelerating away. I think there are three key developments that are going on on a worldwide basis which clearly impact in terms of the UK public sector. The first thing is the web/the Internet is underpinning most major economies and most successful businesses. Most things are something to do with web-based transactions. The second thing that is happening is everything to do with communications—the way we use mobile phones, our fixed lines—is blurring and everything is coming together in a converged approach. The third thing that has happened ever since technology has been invented is it is getting smaller. When you put those things together what is happening is that every technology and every system is available where you are when you want to use it and that fundamentally is changing citizens' outlooks and customers' outlooks in terms of what they see as the normal service that they expect. It is

not a service for our convenience; it is a service for their convenience, and those things are happening in every walk of life. That is where I see the big technological changes coming, the whole Internet, the whole convergence of technology, and wherever you are technology is moving, as we have heard in this room this morning, with mobile phones, et cetera.

Q399 Bob Russell: Mr Suffolk, there are a lot of people out there who are technology challenged and I do represent the technology challenged. Where do we fit in in this great brave new world?
Mr Suffolk: I think that is a very good question because we do sometimes lose sight of the fact that the Internet in terms of the UK has just over 60% penetration and so not everybody does use the Internet, but it is not necessarily the people that we would think about. There are some people who do not have access to that technology. Our starting point in terms of technology is first of all what problem are we trying to solve or what is it that citizens want. Then we are looking for what solutions best solve that problem. Therefore our belief is—and this is the work we are doing with David Varney as part of the Transformational Government strategy—that one route for dealing with citizens is not acceptable. Some citizens will always want face-to-face service; some will want telephone services; some will want Internet; some will want all three. Therefore it is very important that we do not disenfranchise any section of the population by going down one particular route.

Q400 Bob Russell: So I can be satisfied that I as the technology challenged Member of Parliament for Colchester will not be discriminated against?
Mr Suffolk: Absolutely.

Q401 Bob Russell: Thank you. How does the CIO Council ensure that where possible technology-based systems are not duplicated? How is information on the development of systems shared across government?
Mr Suffolk: One of the processes I have put in on the CIO Council is a process called the champion/challenger process. It is fair to say that the public sector has vast amounts of technology and we do not always see where that great technology is and we run the risk of reinventing the wheel which increases risk, increases cost, and slows our time from a citizen outcome perspective. The champion/challenger process is a very simple process. Anyone can nominate a champion. Let me give you an example. The Government Gateway, where we have 12 million citizens and businesses registered so they can get access to government services—someone can come along and say, "I believe that is a champion asset." Anybody can come along and say, "No, I think I have got a better one," and therefore it is quite democratic in terms of the way we do this. An evaluation process occurs and the best product will commence. The rule is quite simply this: if you cannot beat it, you should join it. It is a peer-based review, it is very democratic, it does not take a long time to do, but the objective is to begin to coalesce the systems and technology that we have already in the public sector that we can continue to invest in and protect and support without having to go through connecting 23 different systems together. That is a long-term activity but it is also the right way of doing things. The CIO Council runs that process.
Bob Russell: Thank you, Chairman.
Chairman: Thank you very much, Mr Russell. Gwyn Prosser?

Q402 Gwyn Prosser: Mr Suffolk, one of the strands of the Transformational Government Strategy, as you know, is shared services and common infrastructures, which includes a reduction in the number of computers storing data and networks, et cetera. It seems on the face of it perhaps a logical progression but we have heard from a committee of Dutch experts that their recommendation in their country to move towards a single clearing house for data was met with huge opposition on the grounds that greater centralisation could result in a greater threat to security. What is your view? Where is the balance to be struck?
Mr Suffolk: I think you are absolutely right; there is a balance to be struck. First of all, I think it would be nonsense to assume or even think about a central database and a central clearing house. The UK public sector is more advanced than many countries because we have been doing joined-up technology for years. The oldest computer system that I know in the public sector is 33 years old on 1 April 2008, which is the Police National Computer, and therefore we work at a national scale, and when you work at a national scale I think to continue to put more eggs in a single basket is a foolhardy approach. You are absolutely right when you say that some of the best ways of protecting data are to say that this data has a specific purpose, the purpose is clear in terms of all parties, and therefore we can put protection around that specific purpose in terms of only the people that need legitimate access to that data can access that data. The more and more we put it into large databases where more and more people have access to it, it becomes more complex. I think there is a balance to be struck, but clearly what we want to avoid doing is creating yet another large-scale citizen database when we have a number of those already because that would not be a wise thing to do.

Q403 Gwyn Prosser: Ms Moriarty, the passage of the Serious Crime Bill represents a good example, some people say, of cross-government working on data-sharing. If that is your view, what was done right during that exercise which made it such a success and what could the Ministry of Justice learn from the exercise?
Ms Moriarty: It is a very good example because fraud as a crime is obviously an area where information sharing can be of great benefit. What was specific about the Serious Crime Act was that the information that needed to be shared was relatively sophisticated and relatively sophisticated

arrangements were needed because of the nature of fraud as a crime, and that meant the protections that needed to be in place were also more complex than in some areas. What happened with that piece of legislation was the Ministry of Justice worked very closely with the Home Office in framing the legislation which provides a legal gateway through which public authorities can share data in order to prevent fraud. There was a lot of discussion between the two departments and with the Information Commissioner on exactly what was the best way of achieving the policy objective. As the legislation went through Parliament there were a number of changes made, particularly the introduction of the requirement for a Code of Practice. It is a good example of spotting the issue, working together between departments and with the Information Commissioner to find the best way of addressing that issue, making sure that we have the right powers in place to do it and also listening to the views of Parliament and being prepared to make amendments as the legislation goes through.

Q404 Gwyn Prosser: How will the Ministry of Justice work with the Information Commissioner to take forward the Framework Code of Practice for Sharing Personal Information?
Ms Moriarty: The Information Commissioner has published the Framework Code of Practice and we very much support that as a way of encouraging public authorities to develop Codes of Practice and giving them a template to work with. We will be working with him and with the public authorities as they develop their Codes of Practice.

Q405 Margaret Moran: You will be aware that the Varney report referred to engaging citizens, businesses and the private sector in both the design and delivery of services. Referring specifically to Clare at this moment, how can you assure citizens that the data-sharing that requires is done in such a way that gives them confidence to be able to access those services? Is it not true to say that a great deal of what is good in Transformational Government is data sharing by stealth, in other words local authorities, for example, are doing some of this Transformational Government public service delivery but they do not want to tell anybody because the data-share rules are so obscure?
Ms Moriarty: To take the first part of the question, public trust and confidence is one of the biggest challenges that we face. We know from research which Ipsos MORI did that the vast majority of people want to see more sharing of information in order to produce better and more joined-up services, provided that the right controls are in place around the data. The Information Commissioner published his tracker survey last week and that showed us that people are very concerned that their data is properly protected and they are very concerned about the sorts of things that might happen to it. We are not seeing a huge groundswell of people who are really concerned that organisations are not looking after their data properly but they do feel they are losing control over their data and they want more reassurance that the legislation and the operational practices are going to provide, and are going to continue to provide, adequate protection. That is why, while we are confident that the basic architecture of the data protection, data-sharing system is robust, we have to keep looking at it as the technology moves on, as people's expectations move on, so we need to be making sure that it is constantly up-to-date. That is something we do all the time internally and we have also recognised the need to have some independent input to that process and that is why we have set up the independent review which Richard Thomas[2] and Mark Walport[3] are going to lead looking at the use of information in both public and private sectors.

Q406 Margaret Moran: I also mentioned the fact that people are doing data-sharing by stealth in the public sector.
Ms Moriarty: I am not aware of any detail about that.

Q407 Margaret Moran: Local government?
Ms Moriarty: Broadly speaking, as I said, the Framework is that there has to be a purpose in order for data-sharing to take place, there have to be the correct powers in the place, there has to be an assessment of the proportionality and the data has to be properly protected. As long as all of those things are in place then it is reasonable for people to share data, but if they are sharing data without the powers then that is something which is an issue that we need to take up with them and the Information Commissioner.

Q408 Margaret Moran: Perhaps you would like to comment on that, John, but can I ask you particularly, what is your role in ensuring that government departments do engage with the public when they are developing Transformational Government services and sharing personal data? Could you comment on the fact that when we spoke to the head of the Social Inclusion Unit recently she made the comment that the issue around data-sharing and privacy is very much a middle class concern rather than a concern of those who need those services at the frontline.
Mr Suffolk: Thank you. There are three points there. The first one is that I am not aware of anyone sharing data on stealth. The question was asked if we sometimes get in and arbitrate deals with departments and the answer is, yes, we do and frequently that comes around people's interpretation of "Do I have the powers to data-share?" All of my experience when I work across local and central Government is that people are very conscious in terms of data-sharing, very conscious in terms of do they have the powers and do they have a legitimate purpose. I am absolutely not aware of anything occurring by stealth, as Clare has already

[2] *Note by Witness*: Richard Thomas is the Information Commissioner.
[3] Note by Witness: Dr Mark Walport is the Director of the Wellcome Trust.

said. If we knew that then we would go in and work with the teams and understand why that has happened.

Q409 Margaret Moran: Do you talk to SOCA teams?
Mr Suffolk: I am very happy to talk to SOCA and I will take it up with our colleagues in SOCA. In relation to the second point, which was engaging citizens to understand what they want, as part of the Varney work in terms of Transformational Government, which is putting the citizen at the heart of what we do, we have created a thing called the Customer Insight Forum and the objective there is to share information about what citizens' wants, needs, likes and dislikes are because, of course, citizens come to us in different guises and that is why we have created things like Customer Directors, one for old people, one for farmers, and of course you could be an older person and a farmer. The purpose there is to say, "Let's look through the eyes of the citizen and understand what their need is and what the best way of delivering that need is." It is fair to say historically that we have not always been as good as we could have been in terms of sharing that insight, hence why we created the Customer Insight Forum and why we have positioned that knowledge, that information, at the heart of the way that we do service design. We are absolutely conscious in terms of we have to look at it through the eyes of the citizen and we have the processes on board in terms of doing that. Your point about data-sharing and security being a middle class view, I have heard that said before and those who want a benefit would say, "Guys, share my data to give me the benefit". Our starting point is really quite simple: what is it that we are trying to do with the citizen, what is their need? If their need, for example, is giving benefits quickly then the systems and the programmes that we have designed are around fulfilling that requirement. We never look at this from a one-size-fits-all point of view in terms of, "Here is an approach which will apply to all walks of life", it fundamentally does not work that way. Customer insight mapped on to what is the purpose and what problem are we trying to overcome from the citizen's perspective should drive whatever solution and technology that we put in place.
Chairman: The final question is from James Clappison.

Q410 Mr Clappison: Could I ask you both if you would comment separately from your points of view to tell us if you track trends and new developments relating to data-gathering and data-sharing? One example which has had a bit of publicity in the past is the use of loyalty cards which give businesses a great deal of personal information about shopping habits and, perhaps even more topically, the growth of social networking websites, which the younger generation know all about but I have got to say I do not know all that much about.
Ms Moriarty: From the Ministry of Justice, we work with all government departments who in turn work with the various sectors that they connect with, so within each sector departments will be gathering information and looking at trends. We also work closely with the Information Commissioner. We have complementary roles. We are in charge of setting the Framework, he is in charge of regulating it and, obviously, as the regulator he can gather evidence about all the sorts of issues that are coming up, and certainly social networking forums is one of the issues that he has identified and he is working on guidance to make sure that people understand the basis on which they are giving their consent, that they know what might happen to the data. It is something where we work, as part of our work across Government, with departments and the Information Commissioner.

Q411 Mr Clappison: From your point of view, given the difference of roles between yourself and the Commissioner, have you seen anything in trends in the social networking sites, some of which are obviously well-known, which concern you or are of interest to you?
Ms Moriarty: It is one of the issues that make us aware that we constantly need to be looking at the Framework to make sure that it is up-to-date, and that is something we would expect the Thomas / Walport review to be looking at because it covers the crossover between the public and private sector.
Mr Suffolk: We certainly do track all of the social networking and the trends in terms of what people are doing and we do this for a number of reasons. The first reason is in terms of what are people's perceptions in terms of security and personal privacy. We ran the Get Safe Online Week last week and all the research is telling us that still we have 20% of people who use technology on the Internet who do not have basic protection. Of the 80% who do, 50% do not keep it up-to-date. When you translate that on social networking, those behaviours are often translated as well, so people do give out their date of birth and personal information which, of course, is a primary cause and stimulus from an identity theft perspective. Often we track the technology from the basis of how are people using those technologies and what does it tell us in terms of their propensity to secure themselves or not to secure themselves. Also, if you take something like mySpace, one of the bigger social networking sites, the amount of users on that is equivalent to the eleventh largest country in the world. It fundamentally begins to tell you how the world is shifting in terms of how people treat technology and how they expect service providers and governments to deal with them from a technological perspective, and we track it in that context in terms of what is the norm in terms of the way we are doing business and what are the consequences of doing business in that way.

Q412 Mr Clappison: Could I ask on a slightly separate subject if there are any lessons you think the Government can learn from the private sector in terms of harnessing IT capability?
Mr Suffolk: We partner extensively with the private sector and much of what we do from a technological perspective is outsourced to the private sector.

Clearly we are working at a scale which is much bigger than the private sector from the number of countries that we deal with, because we operate in 148 countries now, and we work at a level of security the private sector would not need to worry about because we have to protect loss of life, witness protection, domestic violence, et al. Where I think the private sector is exceptionally good is how do you create customer facing worlds that absolutely map on to their hopes, their aspirations and their requirements in a quick way and, therefore, there is always learning that we look to take from the private sector. We also work extensively with every major supplier from around the world because, rightly or wrongly, I have a belief that somebody somewhere in the world has cracked most of the problems, we just do not know where they have cracked them. One of the roles that I am more used to is to act as a kind of data agent where someone says, "I have a particular problem, do you know somebody with a solution?" and often those solutions exist somewhere under a different banner in health or education and we try and match those two up.

Q413 Margaret Moran: A small but practical question. I recently visited my CCTV hub in Luton and they have been the subject of some publicity because a beating up in the town centre was relayed on to YouTube, I believe. What mechanisms are there to retain the privacy of that data through the whole process so that both the victim and those who are the alleged perpetrators are not identified and, indeed, the integrity of the criminal justice system is not jeopardised?
Ms Moriarty: That is obviously a misuse of data because the data collected by the CCTV cameras is not intended to be used for those purposes, so there is a breach of data use there. We have a system for regulating compliance with the Data Protection Act. One of the things we have recently done is to change the penalties for wilful misuse of data because the Information Commissioner gathered evidence that the penalties were not—

Q414 Margaret Moran: I am talking about the process, the trail of that.
Ms Moriarty: The trail of process?

Q415 Margaret Moran: The data is shared across a number of actors within the criminal justice system from the CCTV operator to it ending up on YouTube, but there were a lot of actors in-between.
Ms Moriarty: It depends on what data-sharing arrangements are in place, but the data-sharing arrangements all have to be governed by the provisions of the Data Protection Act, so there has been a breach and if it is a breach which is significant then that is something which needs to be investigated and, if necessary, prosecuted.
Mr Suffolk: If I could just come in there. It really comes down to what Richard Jeavons said this morning. The more and more that the technology becomes sophisticated, we absolutely will be able to find people who are getting access to systems and using information illegally. In that instance where clearly they have breached the Data Protection Act by taking data and using it for a purpose that it was not intended, there will be audit logs in terms of who had access to those systems. My belief is that we have to execute that review process to find out what went wrong in a situation like that and learn those lessons because it is clear that is not what should have occurred.
Chairman: Mr Suffolk, Ms Moriarty, thank you very much for giving evidence today. We have almost concluded our evidence for our report into the Surveillance Society. Our next evidence session on this will be on 11 December when ACPO and the Minister at the Home Office, Tony McNulty, will be giving evidence.

Tuesday 18 March 2008

Members present:

Keith Vaz, in the Chair

Tom Brake
Ms Karen Buck
Mr James Clappison
Mrs Ann Cryer
Mrs Janet Dean
Patrick Mercer
Gwyn Prosser
Bob Russell
Martin Salter
Mr Gary Streeter
Mr David Winnick

Witnesses: **Assistant Chief Constable Nick Gargan,** Association of Chief Police Officers, and **Chief Constable Peter Neyroud,** Chief Executive, National Policing Improvement Agency, gave evidence.

Q416 Chairman: Can I bring the session of the Select Committee to order this morning and refer all those present to the Register of Members' Interests. This is the very last session of our year-long inquiry into the surveillance society and this is an investigation that has taken us to Washington DC to look at the procedures in America as well. We are delighted to welcome as our penultimate witnesses, Mr Gargan and Mr Neyroud. Thank you for coming. Mr Gargan, may I begin with you? You told us that the Review of the Regulation of Investigatory Powers Act identified "a proliferation of unnecessary bureaucracy which was borne of a generally risk-averse approach". What bureaucracy is involved in securing authorisation to use RIPA powers?
Assistant Chief Constable Gargan: Typically, in the case of a directed surveillance authorisation, one would expect to see an application form of about 17 pages when one adds in all the considerations for the form and the risk-assessment and the authorisation itself, which in the view of ACPO is entirely appropriate when we are dealing with cases of directed surveillance in the commonly understood sense of the word, but our contention is that that has been inappropriately applied to scenarios where, for example, officers might turn a CCTV camera round to focus on a parade of shops or we might offer the victim of racist graffiti a camera in their own home to film people offending against their own home, and our sense is that this is potentially a sensible piece of legislation that has been the subject of over authorisation, unnecessary authorisation and, as a consequence, unnecessary bureaucracy.

Q417 Chairman: How does your experience compare with colleagues in other countries who have to seek judicial authority to carry out surveillance?
Assistant Chief Constable Gargan: I think in other countries the experience tends to be that the authority is more wide-ranging; therefore an investigation might be authorised rather than a specific suite of tactics. One of the things that frustrates colleagues in the UK is that, on an action-by-action basis, separate authorisations are called for. We have seen progress made in the field of Comms-Data (Communications Data) where we can now have a general authorisation within and under the ambit of which separate activities can take place, but at the moment we still have a situation where for surveillance and other covert tactics within an on-going investigation you need a succession of individual authorisations. That, again, is arguably unnecessarily bureaucratic.

Q418 Chairman: Is not a risk-averse approach wise when unauthorised or misdirected surveillance can have serious consequences for individual liberties and privacy?
Assistant Chief Constable Gargan: We do not advocate a reckless approach at all, we have a sense that risk-aversion does have its place when you are dealing with techniques that really do risk infringing on people's liberties, so they are at the top end of surveillance, of covert investigative techniques, powers under the Police Act and intrusive surveillance under RIPA and, indeed, long-term directed surveillance. It is absolutely right that we should have rigorous controls in place, and they are there. Our argument is that we are effectively dressing up routine law enforcement activity as covert surveillance and over-authorising in those circumstances. It is entirely unnecessary, for example, in the case of sending a teenager into an off-licence to buy alcohol as part of a test purchase operation. In recent years it was common practice to have that teenager registered as an informant, as a "Covert Human Intelligence Source," until common sense prevailed and the Home Office sent out a circular to say "This is nonsense". That is the type of ground that I think we should take and claw back that ground and say, "if it is routine controlling activity, let us not write 17 pages of bureaucracy about it, let us just get on with it".

Q419 Tom Brake: I just wanted to check on that point about the 17 pages long form that has to be filled when in you turn the CCTV camera round. That is not because people are interpreting the law in an over cautious way; that is an actual requirement.
Assistant Chief Constable Gargan: That is a moot point. There are those in ACPO who would say that if you focus in on the definition of directed surveillance and section 26 of RIPA, it is about obtaining private information about a person and it is about covert surveillance. I would personally

seldom authorise that activity, on the basis that the camera tends to be on the top of a very large stick which has got a "CCTV camera" sign on the bottom of that stick. The community is well aware of the presence of that camera. I would argue both that it is unlikely to be covert and that it is unlikely to result in the obtaining of private information, but we have failed to achieve a consensus about that interpretation. Within ACPO and with the support of the National Policing Improvement Agency, we advanced a document containing 20 principles, 20 scenarios, where we felt authorisation would be the exception rather than the rule, and whilst we have the support of the DPP and the CPS for that document, we have been unable to agree its content with the Chief Surveillance Commissioner and, as a consequence, the document is currently in the sidings and that work and other work in connection with the review of RIPA has been referred back to the Police Minister. We anticipate and look forward to a positive response to that referring back to the Police Minister and we would like to see clarification.

Q420 Patrick Mercer: Mr Gargan, what is the extent of the problem of unregulated surveillance by organisations other than the police?
Assistant Chief Constable Gargan: It is impossible to say, because it is unregulated and there are no records. In the submission we observe that, whilst our activities are very tightly regulated, as are those of other public authorities, there is no offence of unlawful surveillance, and private individuals, commercial enterprises, are free to conduct surveillance as they see fit with really only the laws around harassment and data protection to control their activities.

Q421 Patrick Mercer: I hesitate to talk about more legislation, but do you think that we need more legislation to facilitate prosecutions for misuse of personal data and surveillance techniques in the private sector?
Assistant Chief Constable Gargan: That is a matter for Parliament. All that ACPO observes is that there does appear to be an imbalance between a very tightly regulated public authority sector and an almost entirely unregulated private sector.

Q422 Patrick Mercer: The other side of the coin is that the police might be better equipped to detect and investigate crimes such as identity theft.
Assistant Chief Constable Gargan: Indeed, but one of the arguments about unregulated surveillance is that on occasions the two meet: the classic case of the under-cover reporter who may, for example, blunder into an existing investigation, putting themselves and the investigation at risk in a manner that is pretty much entirely unregulated.

Q423 Chairman: Mr Gargan, you have read the Rose Report.
Assistant Chief Constable Gargan: I have.

Q424 Chairman: What lessons can be learnt from the Rose Report?
Assistant Chief Constable Gargan: I think the Rose Report represents a very positive outcome for the Police Service in that, in section 17 of the report, Sir Christopher Rose finds that all the appropriate procedures were correctly followed throughout.

Q425 Chairman: Without referring to any on-going prosecutions or investigations, it was, of course, your force that put the surveillance equipment in the prison. Is that correct?
Assistant Chief Constable Gargan: That is correct, yes.

Q426 Chairman: Did you authorise that?
Assistant Chief Constable Gargan: No. I was not in the force at the time.

Q427 Chairman: Was it another senior officer?
Assistant Chief Constable Gargan: I think the Rose Report refers to a range of authorisations, some of which were granted within Thames Valley Police, some of which were granted by other police forces.

Q428 Chairman: There are no lessons in particular that you feel can be learnt from the experience?
Assistant Chief Constable Gargan: I think that the primary lesson relates to the media coverage of the Wilson doctrine. We have had an opportunity to reflect within ACPO and within, specifically, the ACPO crime business area on the Wilson doctrine and have agreed that we will learn something. I think, looking around ACPO, actually very few ACPO colleagues were even aware of the Wilson doctrine at the time of the media coverage.

Q429 Chairman: But you are now.
Assistant Chief Constable Gargan: We are now.

Q430 Chairman: So what are your reflections on the Wilson doctrine?
Assistant Chief Constable Gargan: Four things. The first thing is that it is helpful to clarify that the Wilson doctrine applies only to those covert activities requiring ministerial authorisation; therefore property interference and intrusive surveillance, when carried out by police forces, are in our view not covered by the Wilson doctrine. Secondly, we believe that adequate provision exists within RIPA to ensure that an individual's privacy is respected and that considerations of necessity, justification, proportionality, collateral intrusion, et cetera, are taken into account when authorisations are made. The third point we would make is that ACPO is broadly supportive of the suggestion made by the Interception Commissioner in 2006 that the Wilson doctrine should be abolished and, if it is necessary to put it in legislation, then let us put it there or, indeed, in a code of practice rather than having this separate doctrine. Finally, the discussion around the Wilson doctrine has uncovered a technical defect in RIPA, in that RIPA makes no

mention of confidential information, and that serves to strengthen the case for a revisiting of the legislation and a revision of the Act.

Q431 Chairman: So, in the end, the Rose Report does provide us with an opportunity to look at this whole area again?
Assistant Chief Constable Gargan: Indeed, and in my view it is an excellent report, very helpful and provides a further spur, if one were needed, to revisit the legislation.

Q432 Chairman: As far as you are aware, is there continued surveillance in prisons authorised by your force?
Assistant Chief Constable Gargan: Yes.

Q433 Chairman: It is going on at the moment?
Assistant Chief Constable Gargan: I am unaware at the moment, but as a matter of general policy, surveillance in prisons continues to take place. In terms of the very specific question of directed surveillance against Members of Parliament, it is my understanding that in the last four years there has been no directed surveillance authorisation specifically targeting a Member of Parliament, but in terms of surveillance in prisons, yes, it does continue and will continue.

Q434 Chairman: So if a Member of Parliament visits a constituent in prison who happens to be the subject of surveillance, that surveillance will continue. It will not stop because a Member of Parliament visits a constituent.
Assistant Chief Constable Gargan: It depends on the nature of the authorisation, the nature of the visit and the circumstances in which the Member of Parliament were to introduce themself to the prison.

Q435 Tom Brake: On Sir Christopher Rose's report on privacy of communications, he makes it very clear that after 2005 there has been no recording of privileged conversations, but he was quite specific in saying "after 2005". Are you aware, were there any before 2005?
Assistant Chief Constable Gargan: I am not. I do not know the answer to the question.

Q436 Martin Salter: Can you clarify for me, Mr Gargan, because, as I understand it, the police are prevented from undertaking surveillance if a prisoner is seeing his or her solicitor but not if a prisoner is seeing is or her Member of Parliament. Is that correct?
Assistant Chief Constable Gargan: That is correct. They are not prevented; it is just that special provisions apply. This is confidential material subject to legal privilege and special provisions apply.

Q437 Martin Salter: To lawyers?
Assistant Chief Constable Gargan: It is a higher level of authorisation, and a higher level of authorisation and protection does not apply in law to interactions between a prisoner and their MP. The effect of the Wilson doctrine, were it to be applied to surveillance, would be to afford a higher level still, but in our interpretation the Wilson doctrine does not apply to surveillance and, therefore, this would not apply.

Q438 Martin Salter: You made it perfectly clear that the Wilson doctrine does not apply to police surveillance in respect of a Member of Parliament visiting his or her constituent in prison. Do you think it should? Do you think that a prisoner has a right to have a privileged and confidential conversation with his or her Member of Parliament as well as his or her lawyer?
Assistant Chief Constable Gargan: I do not have a view on that. That is a matter for Parliament. It would be a reasonable thing for Parliament to decide to do, but I do not think my view is of any particular value.

Q439 Mr Winnick: If I understood you correctly in your answer to the Chairman, if a Member of Parliament visiting a prisoner lets it be known, if it is not already known (and presumably it would be) that he or she is a Member of Parliament, then there would be no interception?
Assistant Chief Constable Gargan: No. If a Member of Parliament were to visit a prisoner and makes it clear that he or she is a Member of Parliament and the nature of their visit is in relation to their business as a Member of Parliament, their constituency business, there would still be no extra protection afforded by the law. Our view is that the Wilson doctrine would not cover that because we are talking about surveillance here, either directed or intrusive surveillance, and not covert activity as authorised by the Secretary of State, and that covert activity authorised by the Secretary of State would amount to telephone interception, which would not apply in the circumstances.

Q440 Mr Winnick: The case of a colleague of ours, Mr Khan, could repeat itself when that conversation he had with a prisoner was monitored?
Assistant Chief Constable Gargan: It is entirely possible, yes. Ultimately, I think the misapprehension about the Wilson doctrine was that it applied to surveillance, when it has never applied to surveillance, so it would be a matter for Parliament to create a protection. Our view is that the legislation itself creates protections for all interactions.

Q441 Mr Winnick: It does somewhat undermine the confidentiality between a Member of Parliament and a constituent, does it not? That is not your view.
Assistant Chief Constable Gargan: That is a matter for Parliament.

Q442 Chairman: I have one final question before we move on. This was a Thames Valley operation, clearly, and Thames Valley officers were involved in the surveillance of this particular prison. Is that right?

Assistant Chief Constable Gargan: I think Thames Valley officers were involved in the surveillance but it was not a Thames Valley operation. I am reluctant to go further into that because, as you are aware, there is an on-going case.

Q443 Chairman: Who would have the tape-recording of this conversation? Would it be Thames Valley or someone else?
Assistant Chief Constable Gargan: I do not know the answer to that. I think that would depend on the circumstances of the case.
Chairman: Thank you for answering those questions. Let us move on now to CCTV cameras.

Q444 Mr Winnick: Mr Gargan, most of us have been arguing for CCTV cameras in our own constituency, and you say in your report that they help in the investigation of crime. Yet, at the same time, a recent joint work with the Home Office showed that 80% of CCTV images are "far from ideal". Does that not somewhat contradict the positive work which CCTV cameras are supposed to do in undermining crime?
Assistant Chief Constable Gargan: I think the case for CCTV cameras is compelling. As a senior investigating officer myself, or rather, a former senior investigating officer and somebody who supervises senior investigating officers, I am well aware that very often the very first investigative action, or one of the very first investigative actions that takes place in virtually any serious crime inquiry or missing person inquiry or many other types of inquiry would be to conduct a trawl of CCTV evidence and see what that tells us. It is an indispensable investigative tool.

Q445 Mr Winnick: We accept that, but at the same time, as I have said, 80% of such CCTV images are far from ideal. This is from the joint report with the Home Office?
Assistant Chief Constable Gargan: That is right, and so the Home Office and ACPO have collaborated on a strategy to drive up the standards, and my colleague, Deputy Chief Constable Graeme Gerrard, from Cheshire, is the ACPO lead on that strategy. It makes 44 recommendations that envisage a gradual upgrading of facilities and a convergence of facilities towards a technical standard, and we will, I hope, see an already very useful technology become more useful still.

Q446 Mr Winnick: Without going into those 44 recommendations—timewise it would be difficult—you are rather optimistic that these cameras can be improved substantially?
Assistant Chief Constable Gargan: Yes, we are optimistic. The technology is already excellent and indispensable and the strategy is sensible and will move us forward.

Q447 Mr Winnick: You query the statistics on the number of cameras in place. Why is that?
Assistant Chief Constable Gargan: We hear the figure 4.2 million cameras quoted very regularly. My understanding is that that 4.2 million is an estimate based on a study which dates back to 2002. The study looked at the number of cameras found on Putney High Street in London and then did a quick calculation and extrapolated that, as a consequence, there must be 4.2 million across the UK; so we approach that figure with some scepticism, although it is widely quoted.

Q448 Mr Winnick: What sort of figure should we, in your assumption, work on?
Assistant Chief Constable Gargan: I do not know. I think what we do know is that there are around 30,000 Local Authority operated street cameras, and they are the ones that the strategy focuses on specifically and particularly.

Q449 Mr Winnick: You remain convinced that they are a very useful weapon in the fight against crime?
Assistant Chief Constable Gargan: Absolutely. The theme of the ACPO submission is that the suite of covert and overt surveillance tactics that are available to us are fundamentally important, and the position of ACPO is that they really must be defended and made accessible to us.

Q450 Mr Winnick: You work, again, presumably, on the assumption—without putting words into your mouth—that the only people who should fear them are those who engage in criminality?
Assistant Chief Constable Gargan: I think that is a very sensible summary and one that I would be happy agree with. I should add that we should be able to make use of overt Local Authority CCTV with the minimum bureaucracy, because everybody knows it is there and we should not be hampered in our use of it.

Q451 Bob Russell: Chief Constable, I would like to ask a few questions about facial images and developments in technology. What role does the National Policing Improvement Agency take in terms of the development and deployment of new technologies such as automated face recognition?
Chief Constable Neyroud: We are the single national support to the Police Service in developing not just this technology but the other aspects of science and technology for the Police Service. I have a biometric and identification team that are providing the national programmes and national support, including, incidentally, the last issue, CCTV—we are dealing with the CCTV strategy as well—and so we lead on this development nationally and we work very closely with a range of other parts of government as well.

Q452 Bob Russell: Is this team self-contained or does it bring in officers and experts from around the country from time to time?
Chief Constable Neyroud: Very much the latter. The Agency has got a range of staff drawn from civil servants, public servants, science and technology specialists, seconded police officers, seconded from local authorities, et cetera. We draw very much from expertise in the field.

Q453 Bob Russell: Joined-up thinking?
Chief Constable Neyroud: We try.

Q454 Bob Russell: How do these new techniques measure up against more traditional policing in terms of the prevention and investigation of crime?
Chief Constable Neyroud: Let us be specific about the techniques. There is a range of things within FIND, which is the Facial Image National Database programme, the first of which is (back again to the issue on CCTV) single national standards so that we are all using the same standards and can share them. The second issue is getting facial images available to the Police Service that can match up with the nominal records. That is a programme that we are moving in slightly slower time because we do not think that is going to give us the major move forward at the moment. I am happy to develop that. Then we have got facial recognition techniques where, if those are applied on small local databases where you are not dealing with huge numbers of facial images, they can be very effective in narrowing down the identification, but that technology is also moving on to the next stage, which is behavioural matching, the ability to pick out odd behaviours in a crowd—for obvious reasons, this might be particularly powerful in the case of counter-terrorism or a variety of street crimes—and that is about watching for movement in a wider crowd. Those technologies are moving quite quickly and being developed.

Q455 Bob Russell: In your memorandum to us you say that "we", society, are now accustomed to being monitored by cameras and the public expects CCTV footage of criminal activity to be available as a matter of routine. Apart from the criminal fraternity, who may prefer not to be monitored in this way, are the concerns of others to be dismissed altogether?
Chief Constable Neyroud: No, not at all, but, because I was walking to this event, I actually counted, not just the number of cameras on the way from where I was staying over night to the House today, but also the number of messages that make it absolutely plain that the camera is there for a purpose, and the purpose is to prevent crime, and there were over a dozen in half a mile. I think it is very much part of the pattern of society that we now expect that to be protecting us. What we also need to have an expectation of is that the standards that lie behind it and the quality that Mr Winnick referred to is to the highest standards as well. It is all part of the piece of being able to explain what it is there for, what its effectiveness is, how we are looking after it, whether the standards are moving on, the techniques that we are applying and who is applying them.

Q456 Bob Russell: Gentlemen, are public expectations for surveillance cameras too high?
Chief Constable Neyroud: In an odd way I think they are too low. I do not think the public really understand how effective they are in the investigation of crime. I do not think we have done enough research on the effectiveness of CCTV in detecting serious crime. Our guesstimate, on a very short piece of work that we did with one force, is that we are getting almost as many detections, either directly or indirectly, from CCTV as we are getting from DNA and fingerprints. It is a hugely important part of serious crime investigation. You can tell that from watching *Crimewatch*, in a sense, because you can see so many of those images being deployed. You could also tell from recent missing person inquiries just how absolutely crucial CCTV is in helping the police to identify and find vulnerable missing persons, and you could see from our set-up that we are also responsible for the National Missing Persons Bureau. We see CCTV as a crucial part of that.
Assistant Chief Constable Gargan: I think that any perception on the part of the public that there is some kind of Orwellian infrastructure sitting behind society where these cameras are terribly well integrated and joined up as part of a surveillance state is entirely wrong. Actually, I saw some reporting in the wake of the debate about Woodhill which sought to infer that somehow every local authority, every shop CCTV camera is somehow networked. That is very wide of the mark indeed.

Q457 Bob Russell: The opposite of the Orwellian state is perhaps the same as safety measures in cars (seatbelts): there is a thinking that perhaps people are more casual and less determined to be a safe driver. Is there a danger that if people assume that public spaces are under constant surveillance by the police, they will pay less attention to their personal safety?
Assistant Chief Constable Gargan: Having spent many a long and, frankly, boring hour watching CCTV coverage live in town centres and city centres, it is amazing how little impact they seem to have on the behaviour of all but a very few individuals who are very conscious of the cameras and play up to those cameras.
Chief Constable Neyroud: I think one of the crucial things that is often missed in the studies is that if one of the things that CCTV does—and I think there is quite reasonable evidence in the study—is to encourage people to use public space, they create a capable guardianship of that space simply by their presence. Therefore, creating that confidence is actually in itself a crime reduction measure.

Q458 Tom Brake: I am very disappointed, Mr Gargan. I thought that everything that was in *Bourne Identity* was for real, but obviously I was wrong! On the issue of CCTV, can you tell us what could be done to improve the handover of CCTV data, because (and I am sure colleagues have experienced the same thing) when there is a crime, we know there is a camera nearby and there is always an issue about obtaining that data from the local authority. What could be done to improve that process?
Assistant Chief Constable Gargan: I think the ACPO strategy caters for that in terms of taking that process and putting it on an electronic footing and, ultimately, the electronic transfer of data will be an aspiration further down the line. We need to achieve

that in circumstances that maintain the evidential integrity of that product so that we can produce it with confidence at court, and I think the strategy caters for that. It is a work in progress.

Q459 Mrs Dean: Could I ask both of you: what effect do you anticipate that the sharing of bulk ANPR data will have on rates of offences brought to justice both inside and outside the congestion charging and road pricing zones?
Chief Constable Neyroud: The first most important thing as the base of this is just how significant ANPR has been in raising the effectiveness of officers dealing with mobile criminality, and also, incidentally, I do not think there is enough emphasis on dealing with those more serious road offenders who are most likely to commit serious offences. They are just the people who are uninsured, disqualified, et cetera, that we can take off the roads, extending that framework and allowing us to focus on more routes and more roads. As long as we are targeted, and this is the critical thing that between ACPO and NPIA we need to make sure we are getting it right and we are rolling out an assisted implementation programme on that basis. It is all very well having the data, but you have to have the focus to be effective. You will throw up an awful lot of matches otherwise, without the ability to resource it and so—and this is back to Mr Russell's challenge to me about being joined up—we have to be joined up. It is not just about joining up the data, we have to join up the back office techniques that mean that we are focused and effective and we are picking the right targets and we are being very effective. The work that we have done in that territory around, for example, the Birmingham ring-road with the combined motorway patrol group there linking the ANPR shows that we can be many times more effective with that type of data, we can be getting very high levels of hit rate as vehicles go out, but, of course, if you want to follow through into the offences brought to justice, we, the NPIA also have to streamline the paperwork for summary cases, the back office support, the case and custody system, so that we are not dragging police officers off the street as we get more hits, because otherwise that has in a sense a circular reverse effect.
Assistant Chief Constable Gargan: I have nothing to add.

Q460 Mrs Dean: The Information Commissioner and the Royal Academy of Engineering have argued for public access to surveillance cameras. Would it be feasible to operate public assess webcams or to publish maps which show where cameras are located on the transport network?
Chief Constable Neyroud: There are two sorts of cameras here. If we are talking about the cameras that we are overtly telling the public about because they are the cameras that are surveilling public space, I have less difficulty with that: they are literally openly in public space. If we are talking about the network of ANPR cameras, which are designed to catch people who are doing things that are illegal, to be frank, I am not really up for, from a counter-terrorist point of view, providing Al Qaeda with a camera-free route map and I do not think that is the right way to go. It would certainly diminish the capability and, frankly, given the internet capabilities of some of the organised crime groups, it would apply to them as well. I think it is a worthy idea, but it is not one I feel I could support because it would certainly diminish the effectiveness of the network.
Assistant Chief Constable Gargan: I think there is another valuable distinction there between the camera that is a fixed camera giving a view of a particular location. Several colleagues at the minute are anxiously looking at the webcam of Val d'Isère and other ski resorts to find out whether there is snow there. That is fine. Local authority CCTV cameras are quite a different story, because actually the local authority exercises some control over those cameras. If, for example, the camera in Warwick High Street is focused on a jewellers halfway down the High Street, it is probably doing that for a reason, and that information could be very valuable to the criminal who is thinking about robbing that jeweller later this morning. That type of access would be dangerous and potentially useful to criminals and I think that regulation around that and the prevention of that happening would be sensible; whereas seeing whether it is snowing in Val d'Isère causes me no problem at all.

Q461 Mr Streeter: Chief Constable, a couple of questions on the Police National Database. Given the growing propensity of police officers to sell stories to tabloids every time a celebrity is arrested so that there is a front page splash the next day, it seems—and this is becoming increasingly commonplace—how do you think the people of this country can trust the police to run this database?
Chief Constable Neyroud: I am not sure that I can necessarily agree there is growing evidence.

Q462 Mr Streeter: Does it happen?
Chief Constable Neyroud: It does happen.

Q463 Mr Streeter: What are you going to do about it?
Chief Constable Neyroud: Let me take you through the security structure of PND. Firstly, what is it? It is the joining up of the core databases within 58 police forces, including Scotland. What we are doing is actually joining up the existing information infrastructure so that we have got that data across boundaries. Point number one: it does not make that much difference in terms of the type of risk that you are talking about in that respect. Secondly, what we are doing as we are putting it in is we are definitely hardening up for a range of very good reasons, one of which is that the database is rated confidential, not restricted, and so we have a high level of security and that security comes in several areas. First of all, the physical human security, which I think is the primary one in respect of the question you have asked, which is the counter-terrorism check and continued vetting of the staff within the organisation; the second layer is the physical

security about the devices and how you can access it (so password protection on that); thirdly, there is the role-based access to information (i.e. you only get the information you need for the particular role that you have got); and, fourthly, which again gets into the question you have asked, the ability to go back in and audit and monitor the use of certain checks, et cetera, which I personally, in respect of an officer who was leaking information, have used in a very effective way to ensure that that individual ended up in front of a court. If you put those layered changes in, no, I cannot completely protect, and often the situation is not in the formal sense that you describe, it is the informal sense. We are an organisation that does have a very close relationship with the media, in fact we field most of the media stories most of the time, and there is a positive side to that: you could not publish a local paper without us. The down side of that, of course, is that those relationships can be on occasions, as you rightly point out, a little too strong.

Q464 Mr Streeter: Thank you. That is a better answer than I suspected. The IMPACT programme: how does that ensure that the effect of the PND on individual privacy is appropriate and minimised?
Chief Constable Neyroud: We are only two weeks away from the closure of our consultation on equality impact and privacy assessment. We have had over 600 hits on the web page with the full consultation document. We will be publishing the results of that consultation when the consultation is finished. We have been in very close conversation with the Information Commissioner's staff, and a range of other bodies have already commented on it, and we will be taking, as part of the build of the database, a very careful account of the points that are being made in that process.

Q465 Chairman: On the question of access to the database, what is the rank? At what rank can you access the database?
Chief Constable Neyroud: It is not rank, Chairman, it is the issue of role. The rank is completely irrelevant. The issue is what role have you got, why would you need access to that layer of data, do you only need access to the front end of it—for example, do you only need access to the high level PNC data about knowing whether someone is in the system—or do you need access to the more detailed data, in which case you would have to have the right clearance role and access levels.

Q466 Chairman: Does any other country do it better than us in terms of gathering information and hosting it together? I heard that Poland is one of the countries where all the databases are actually held together in an effective way. Do you know of any other examples?
Chief Constable Neyroud: We have looked at about a dozen examples across the world, one being the Naval Criminal Investigative Service example in the States where they are bringing together a whole range of law enforcement bodies. We have looked at examples in Australia, we have looked at the Japanese example, Sweden, a whole range of them. When IMPACT is actually fully implemented, in terms of its capability and its security levels, which I think is a critical thing which the debates of the last few months have highlighted if nothing else, this will be a world leader in terms of the stretch and capability.

Q467 Mrs Cryer: Chief Constable, I want to ask a further short question about information sharing. How do you ensure that information entered on to national databases is actually correct?
Chief Constable Neyroud: There is a whole series of pieces that come together with that. First of all, we now have a Management of Police Information code of practice with standards sitting underneath it. That was introduced just over two and a half years ago. We, as in the NPIA, have been engaged in a year by year process of tightening the implementation of MoPI, and Nick might wish to talk about what Thames Valley is doing to do that, but it is a standard which ensures not just that the data is entered correctly but is weeded appropriately when it is required and that there are systems and filters in place to ensure that those standards are maintained. With regard to the PNC, every force has to have a PNC steering group which looks at a whole series of issues of data standards and security, and, again, the standards for that are publicly available in the code. There have been concerns around things like the timeliness of data on the PNC and the accuracy of data on the PNC. With regards to that, two things are happening together. First, the national implementation of the case and custody programme, which we have all but finished now—it has been a long slog—which NPIA picked up in April of last year as we started which we have now finished. In the next six months we will be implementing the join-up with the Ministry of Justice Libra system and, therefore, you will be entering results from the court end as opposed to the Police Service double-keying or dual-keying; so we are seeking to reduce double-keying into the system and increase the timeliness of data. With the implementation that we have done, for example, in the Met over the 32 boroughs in the last period of time, we have seen a huge jump in timeliness and accuracy with a national system going in there. If you put that alongside the Management of Police Information standard, I cannot guarantee every item of data will be perfect, but the systems have been significantly tightened up, the standards have been tightened up, the processes have been tightened up and we will continue to work on improving that over the next few years.

Q468 Mrs Cryer: Do you believe that what you are doing complies with the Bichard Inquiry recommendations?
Chief Constable Neyroud: We have got about three-quarters of the way down the list of Bichard's recommendations, and that one I have just described, the implementation of the court join-up, will answer recommendation seven, which is the link up and join up of information. We have re-platformed the PNC, we have got the IMPACT

Nominal Index, which allows child protection units and those who are doing the tight public protection to meet that, we have got the Management of Police Information standard and we are at the moment just coming up in November to the letter, the contract, for the Police National Database, which completes the major recommendations under Bichard.

Q469 Tom Brake: Chief Constable, could we now move on to the National DNA Database. In your evidence you said that the NPIA understands there are improvements to be made in the management and delivery of the National DNA Database. A colleague of yours, Gary Pugh, has recently suggested that a way of improving the DNA database might be to include primary school children who exhibit behaviour indicating that they may become criminals in later life. Would you support that extension?
Chief Constable Neyroud: I have actually gone back and read the original paper that that came from, because that was not a line of policy that I was familiar with. What the paper refers to is the challenges of making sure that we have got the right people on the database at an early as possible stage. There is a level of knowledge and detail now about criminal career history, which would indicate that there are some people who are more likely to offend, in a later database, and that was simply where he got to in that article. There are some really significant ethical issues around that and that is one of the reasons we have now got an Independent Ethics Committee. There would be no way that I would suggest we move ahead in any of that direction without the Independent Ethics Committee and, indeed, some of the recommendations out of the Nuffield Report in this territory informing that debate, because I think the most important thing with the DNA database is being really clear with the public what the purpose of the database is, what its effectiveness is, how well it is being managed and the custodianship of it, how well and independently the research processes are being done, so that the public can continue to have confidence in the way in which biometric data is being managed.

Q470 Tom Brake: Perhaps we can come on to that in a second. You clearly do not think at this moment in time that particular proposal is one that you would support, but are there other ways in which you think the DNA database could be extended in a way that you would currently support?
Chief Constable Neyroud: Yes, not in terms of extending the database but extending its use and deployment, one of those being the work that the Government is taking forward on the Prum Treaty for sharing data, within very specifically and controlled circumstances, with other European countries. If the exchanges we have done with the Dutch have illustrated anything, they have illustrated the importance of us thinking about the linkages, and I could think of several other examples outside that exchange. It is fairly obvious: if we have got millions of Britons travelling to Europe and millions of Europeans travelling to Britain, within that there will be people who are committing serious offences, and we ought to be protecting both our public and those of Europe by sharing data in those type of cases.

Q471 Tom Brake: Can we come back to the issue about how to manage it more effectively? For instance, the consent forms that are now used in relation to volunteers and witnesses when you are trying eliminate people from inquiries, can you explain what people are signing up to and do those consent forms allow people to have their DNA deleted from the database at some point in the future?
Chief Constable Neyroud: There are two layers of consent, one of which is: "I give my consent to you having my DNA to match against the database but not on the database for the purposes of investigating this specific crime and I would like you to get rid of it after that point." The second point is: "I am quite happy for you to put my data on the database." Once you have signed that one, you are signing it to stay on the database. The forms are clear, but I think one of the lessons we learnt a long time ago with, for example, telling victims about the possibility of victim support, is that at the time when you are asked to volunteer a sample you are in a police station, it is an unfamiliar environment and there may well be some pressures on you. You may have just been a victim of crime. What we have been doing as an agency over the last period of time, working with the independent committee, is producing much clearer leaflets, much in the same way as we have done with stop and search leaflets, and these will go in with every pack and will be available to people so that the consent is not just informed but people are clear about what they have signed up to and what the process is.

Q472 Tom Brake: Are you able to say at all what ratio there is in terms of people saying, "Yes, but just for this inquiry", verses, "Yes, I am happy to have my DNA on the database for the rest of my life"?
Chief Constable Neyroud: A significant number of people seem quite relaxed to have their data on the database.

Q473 Chairman: Relaxed?
Chief Constable Neyroud: Relaxed as in they have had it explained to them that the database is not a surveillance database, it is an intelligence database that will only match you to DNA if it comes out of a crime scene, and I think that is an important part, and most people seem quite happy, in those circumstances, to provide their data to the database on a voluntary basis.

Q474 Chairman: I have a constituent who was a "have a go hero"—he intervened in an affray. The police arrived and, not knowing people's role, arrested everybody, took him down to the police station, took his DNA off him and subsequently released him and thanked him for his involvement

but kept his DNA. I have written several times to ask for this DNA to be removed and it has not been. What do you say? My constituent is not relaxed.
Chief Constable Neyroud: Okay. There is a small group of people who are very concerned about it, not least of which we have not, in my view, explained effectively what the linkage is, for example, or the non-linkage, between DNA and vetting and that connection. There is not a connection. I have to make that point.

Q475 Chairman: I understand you have to keep it, but if they have not committed any crime and they would like it destroyed, why is the process so long and prevents them getting it back?
Chief Constable Neyroud: This is an area we are working very closely with the Independent Ethics Committee on to get the right balance between retaining samples that will prevent and enhance investigation of crime and the volunteers and other people coming on to the database being clear about what we are doing, how we are doing it and what the procedures are for removal.

Q476 Martin Salter: Mr Neyroud, in your very helpful memorandum the NPIA draw attention to the fact that the rules on collecting DNA, the PACE rules, are subject to a current review. In your memorandum you sing the praises of the DNA database; you call it a key intelligence tool, you say it has revolutionised detections, secured more convictions, and also helps eliminate the innocent from police inquiries. On the other hand, we have all been written to by Liberty who quite clearly are in favour of limiting DNA retention to those who have committed sexual or violent crimes, or at the very least setting the bar extremely high in terms of proportionality. There was a recent case, Steve Wright in Ipswich, where the DNA, as I understand it, was absolutely crucial in securing the conviction. He had already murdered five women and was likely to murder many more. He had his DNA retained because he stole £40. To me, and to many people, this seems a classic example of why the current system works and why DNA should be retained but, given that your memorandum talks in terms of eliminating the innocent, how far down the road do you think we should be going in terms of a wider DNA database, and, we might as well ask the 64,000-dollar question, would you be in favour of a National DNA Database with certain protections?
Chief Constable Neyroud: The last question is more for the Government than me but I will give you some of the issues that I think ought to go into the decision. I am an admirer of Liberty on many issues but I think on this one they are profoundly wrong. There are many serious offenders who first come to notice with a relatively minor offence or subsequently, and one of my own investigations as a senior investigating officer was detected some ten or twelve years later as a result of somebody committing a minor public order offence in another false area. People do not necessarily follow what people think of as a track of committing a career criminal history in a nice, neat order; people are messy and unconnected sometimes in the type of offending patterns that they commit, and we know that now quite clearly from criminal career history. I do not think that we would be protecting the public anything like as effectively. Many of the 450-odd murders that DNA evidence contributed to have arisen from relatively minor offences—theft, disqualified driving, offences of that nature that have been committed by offenders either before or after, so I think Liberty are plain wrong. If our primary job is to protect the public from death, serious injury, harm and loss, which I believe profoundly it is, then this is a very effective database in doing that. How would we extend it beyond that? I am nervous about extension. My team are responsible for answering your Parliamentary Questions, of which we are answering torrents on the DNA database, for very good reasons. I think the level of debate is healthy, and extending it beyond that needs to be done with huge care and as much consensus as possible, it seems to me, and we have a really very significant duty at each stage of the way to be able to demonstrate the effectiveness of each decision, and provide clear evidence to Parliament in that respect. As to the universal database, I think it is a choice. There is a very profound issue that on the whole many of the offences for which DNA is effective are not committed by women so, if you were going to hold the data on 51% of the population, it would be a profound debate because, let's be frank, men disproportionately commit serious violent offences where DNA might lead to a detection, so you have to be, as it were, disproportionately holding DNA on women for the benefit of trying to catch the men, arguably—a sad fact, speaking as an man—but in terms of whether it would be a good way of doing it there are some significant operational points we would have to overcome in how you would get everybody on to the database. You would have to be really careful about when you did it and what the message was. If it was considered to be very much part and parcel of your duty as a citizen that might be a reasonable way of doing it, but I am nervous about the linkage between the DNA Database and very young children, that would trouble me with my own children in those terms, so getting that process right seems to me to be one that requires considerable sensitivity. Finally, we would have to think about the relative costs. It is certainly totally possible to do operationally; the size of the database would not provide us with a huge difficulty. We hold 57 million names from the DVLA on drivers, so the size of the database is not the difficulty. It is the process of getting on, the ethics of it, and the whole relationship with the citizen needs to be carefully debated.

Q477 Martin Salter: Following that up, quickly, I personally do not think there is a chance at the moment of achieving that broad consensus to move to a national database, even though a case can be made for it. Can you help us in our deliberations by perhaps suggesting a halfway house that could extend the valuable work of the current DNA database whilst stopping short of sweeping up

millions and millions of people who, frankly, do not need to be on it and probably would never need to be on it?

Chief Constable Neyroud: Well, I think at the moment what you have is a profoundly important piece of legislation that allows the police service to put identity at the front end of the custody process. My personal view is that is about the right balances, as it stands, in the sense that you are all—and I think many of you have asked questions in this territory—testing the boundaries of that. I am not convinced there is an appetite to go much further across the piece at the moment. The most important point is being able to extend that relationship in a way that enjoys public confidence with some of our European partners, I think that is where we should be focusing our effort, and that is one of the areas that has fruit in terms of the serious crimes.

Q478 Ms Buck: Continuing on the same line, would it be fair to say that you believe that the database you now have increases the likelihood of a criminal being convicted?

Chief Constable Neyroud: Yes.

Q479 Ms Buck: Is the corollary of that, therefore, that people whose DNA is on the database who have no previous conviction are more likely to be convicted than those who are not?

Chief Constable Neyroud: Well, the corollary is that, if you are on the database and you commit a serious crime, or crime that comes up on the crime scene, then yes, you are more likely to be detected.

Q480 Ms Buck: What worries me about this is if you are on the database because you were arrested and not charged and, therefore, do not have a previous conviction, you are more likely to be convicted of an offence than somebody who has committed exactly the same offence who is not on the database, would that be right?

Chief Constable Neyroud: Statistically yes.

Q481 Ms Buck: I had an example recently of a group of children on an estate in my constituency who were picked up, and some were arrested by the police. They were running away, these children, for an offence that happened on the other side of the borough that they could not possibly have committed, and their DNA has been held and several of them are black. They did not commit an offence. Their DNA is now on the database; therefore, they are more likely to be convicted of an identical offence than another child, probably white in this instance. Would that be right?

Chief Constable Neyroud: That presupposes that they are going to go on and commit the sort of offences --

Q482 Ms Buck: No, it does not.

Chief Constable Neyroud: Statistically you are right, yes.

Q483 Ms Buck: So what does that tell us about the equality implications, because this is generally worrying and raises some interesting ethical questions. We had an inquiry last year into young black people in the criminal justice system, and it found that there was disproportionate likelihood at every single level of the police and criminal justice system to be over-representation of young black people. It seems to me that, if we are not careful, particularly the arrest and no charge element of holding DNA is likely to entrench that inequality. Would you agree with that as a risk, and what should we do about it?

Chief Constable Neyroud: I am not sure proportionately it would increase the risk but I take the point, it is a significant issue. Firstly, in response to the inquiry that you did last year, as one of its early actions the Agency has undertaken some extended work on the equality impact assessment of the DNA database. We are just finalising that and we will be publishing the work, the results and the implications of it. The challenge for that, as you will be well aware from that inquiry, is that the processes which finish with the DNA database on those terms start way further back. It relates to, for example, looking very carefully at the way in which police use Stop and Search, which is also one of the policy and practice areas that the Agency leads on. It relates to the ways in which charging and evidence decisions are made in the police station, and, again, that is part of the work that we have a responsibility for supporting the police forces on, so it is the whole system that has to be looked at very carefully in that respect.

Q484 Ms Buck: I would agree with that, and I know that there was considerable progress made in recent years in dealing with some of those equality issues, but would it not be fair to say that, if you removed the holding of DNA from people who were arrested and not charged, it would immediately pull out one of the foundation blocks really of entrenching inequality in the system?

Chief Constable Neyroud: I do not think proportionately it would make a difference. The issue comes back to how people initially come into contact with the police, and the decisions that police officers make at street level about who and who not to arrest, not about the DNA database.

Q485 Ms Buck: I am not sure it does because, however good the policing and however much further progress you make in reducing inequalities in Stop and Search and all the rest of it, there are always going to be people who are arrested who have not committed the crime. Surely it is a simple way of improving the equality in a system to ensure that people who have not been charged with a crime do not have their DNA on the database, unless, of course, they choose like witnesses to give permission.

Chief Constable Neyroud: No, I would have to disagree with you because all you do is take that total proportion of people off the database; you do not affect the overall equality of the database itself.

Q486 Ms Buck: There are layers and layers in all of that but on this specific issue you are, or we as a society are, choosing to take DNA from people who have committed no offence and who have no choice in this matter. They cannot redress that particular inequality.
Chief Constable Neyroud: Unless there are exceptional circumstances which applies to a small number of cases, yes, but that would not affect the overall proportionality of the database.

Q487 Ms Buck: But we are talking about for the purpose of DNA?
Chief Constable Neyroud: And you would miss some 14,000 offences detected.
Chairman: Would it be helpful if Mr Neyroud could write to us with specific —

Q488 Ms Buck: — numbers?
Chief Constable Neyroud: Yes. I would be happy to help with that.

Q489 Chairman: I have one or two quick questions, and the Minister is outside so I do not want to keep you too long and I do not want to know the details of this, but presumably you have suitable contingency plans just in case there is a massive leak of information from the National Database? Do not tell us what they are, but —
Chief Constable Neyroud: The first is not to have that happen in the first place —

Q490 Chairman: No, but do have you plans in case there is a big leak?
Chief Constable Neyroud: We do.

Q491 Chairman: In response to one of my questions, Mr Gargan, you said you did not know where the tape was of the conversation between Mr Kahn and Mr Ahmad. Would you write to us and tell us who has control of that tape?
Assistant Chief Constable Gargan: I will try and find out.
Chairman: Finally, we would like to pass on through you, as you are both members of ACPO, our condolences on the death of Mike Todd, who has in the past been of great assistance to this Committee and his force was at present organising our visit to Manchester. It was a great loss to the police service and to the country. Please pass on our condolences to all concerned. Thank you for coming; you have been very helpful.

Witness: **Rt Hon Tony McNulty MP,** Minister of State (Security, Counter-terrorism, Crime and Policing), Home Office, **Ms Niki Barrows,** Office of the Chief Information Officer, Home Office, and **Ms Nadine Hibbert,** Head, Covert Investigation Policy Team, Home Office, gave evidence.

Q492 Chairman: Minister, thank you very much for coming. This is the very final evidence session of our Surveillance Society inquiry, which has now been going on for a year and three weeks and we are very pleased to have the Minister here before us. Minister, perhaps you could introduce your officials, so the Committee knows why they are here.
Mr McNulty: On my left is Niki Barrows, Office of the Chief Information Officer, Home Office, and on my right Nadine Hibbert, Head of the Covert Investigation Policy Team.

Q493 Chairman: Thank you. Are you confident, Minister, that the Home Office and its agencies can deliver on the Government's commitment to information sharing between public sector organisations and service providers without jeopardising personal information?
Mr McNulty: I think I am, but I would qualify that in a couple of ways. Firstly, you will know that there are a number of reviews going on and we need to take full account of those reviews, variously the Thomas/Walport, the Cabinet Office and the Poynter Reviews, and a couple of extant Select Committee reports that we need to respond to on the back of those reviews, but I am fairly confident in the light of those reviews and our response to them that we are in the right area of these matters. We do take data protection and the civil liberty side very seriously. Everyone will know that we have to share information for effective government and the overall wellbeing of society, but we must get the data protection right and I think that is what is these assorted reviews will look at. If we need to fundamentally change or look at the whole regime or architecture of data protection, then I think there is a clear commitment across government that we shall.

Q494 Chairman: There has been a recent spate of loss of data, Customs & Excise and other organisations. The Home Office as yet has not been in the news for losing any data, so well done on that, but are you taking extra steps to ensure this does not happen in the light of what has happened with other organisations?
Mr McNulty: We are, not least in terms of the Cabinet Office guidelines after particularly the HMRC loss, and we are looking at particular organisational and structural ways to ensure the greater security of data, starting fundamentally from the premise that, unless there are compelling reasons so to do, people may have access to the data but it is not portable in the sense that was highlighted by some of the data losses, or as and when it is portable it is done so in very secure circumstances. We are also, again, I think increasingly for, and want to get to, a universal position on mandatory encryption and learn the lessons very rapidly from those data losses. Also, thank you very much for the "as yet" in terms of the Home Office in the preface to your question.

Q495 Chairman: We are all touching wood, of course, as we say this but, in respect of the amount

of information that you are gathering from CCTVs, ANPR, the National Identity Scheme and the DNA database, is there a convergence of all this data, and, in allowing for this convergence, because there is a huge amount of data you now have, are you worried about the implications for civil liberties and the privacy of the individual? Are the Government holding so much data and information on its own citizens?

Mr McNulty: Yes, but I think people need to understand that much of it, not all by any means, is very temporary. If you look at ANPR, much ANPR data is invariably on a loop that is written over within days. The notion that somehow every product of an ANPR camera or a CCTV camera or any other aspect of government databases are all in some huge warehouse or shed somewhere with a live feed going in on a realtime basis, accessible to anyone across the State, central or local, simply is not the case. In many cases many of the CCTV cameras you are looking at and observing on the high street are on a sort of digital loop that will last days, no longer. Some go to live feed. For some of the more substantial databases it is appropriate that they are shared across government more and more, and in the light of the reviews and everything else that we are undertaking we can be very clear on the civil liberty side as well as data protection, data security and others.

Q496 Chairman: And there is no reason that you might want to dip into health or children's databases as you want to increase information on people?

Mr McNulty: No, I do not think so, and I do not accept really the starting premise that says that Government want to go fishing every time there is a database. If you go back to the example of ANPR, where that is used in an investigative fashion, it is around very strict search criteria and is not going fishing just for sake of it. I do not think there is any efficient way or policy that would dictate the Government just want to go fishing because we are nosy into assorted databases or the product of other data streams.

Q497 Martin Salter: As I am a very keen fisherman could you find another metaphor? We fish for fish, not data! There is a debate on the use of DNA data and the retention of it, and there is a current review taking place. Can you give us some idea when that review is likely, basically reviewing the 1984 PACE guidelines, to come to a conclusion?

Mr McNulty: Principally in the spring. I say "principally" because one of the emerging themes from the broad review of PACE is that for 20-plus year old piece of legislation it is holding up very well. Where there may be substantial changes to it they will follow from the report in hopefully the spring, certainly before summer. Tony Lake, the previous ACPO lead on forensics, made clear that he thought the PACE Review was an opportunity to look at some of the very serious issues around retaining data on the DNA database, particularly for the under-18s, and other matters such as the vexed issue of whether arrest or charge is sufficient to end up on the DNA database and whether those not convicted should come off the database, so they will be part of the review. I know that others, and it may be an area we should look at, my mind is not settled on the matter, are less than happy that PACE is really the statutory core of the existence of the DNA database rather than more formally put on primary legislation, and maybe we should come back to that.

Q498 Martin Salter: Minister, you will have missed the exchange we had with Peter Neyroud, and we highlighted two aspects; on the one hand we have the National Policing Improvement Agency describing the DNA database as a key intelligence tool, that it revolutionises detection, secures more convictions, helps eliminate the innocent. On the other hand, we have all been written to by Liberty basically saying that DNA data should only be retained for people convicted of sex offences or other violent offences, or at least the bar should be put extremely high, too high to have secured the convictions of some fairly high profile murderers in recent cases. Where do you see the balance of this argument coming down, and do you see eventually this country ever moving towards a national DNA database?

Mr McNulty: I am not convinced by the notion of a universal DNA database. I made the mistake one time on a radio programme, when Judge Sedley reported that he was in favour, of saying I had a good deal of sympathy with the logic of his argument, which about four days afterwards was translated as "Government has sympathy for a universal DNA database", and there is a logic to it but I do not accept it. I think broadly where we are now, notwithstanding the PACE review, is where we should be, and I think on this Liberty are utterly and profoundly wrong, not least because of the cold cases and others that we have since solved—murders, rapes and the most serious of crimes—by having someone's DNA perchance on the database when originally it was only on the database because of very minor offences, so the balance is about right. I take Tony Lake's point about maybe looking at the under-18s' retention and how long you should be on the database for, but in some of the high profile murder cases solved very recently the root—not the sole reason they were solved but the root of their solution lay in, I think, in one case a minor assault and in one case a minor robbery. We have a debate at the moment about whether you should shift towards non-recordable crimes as well as recordable, and whether they should go on the DNA database, and I am fairly agnostic about that and would probably lean towards not doing so rather than otherwise. Notwithstanding what I have said about Tony Lake and the PACE review we are in a reasonable position now.

Q499 Martin Salter: Following that up, is there a case for deep bureaucratising of the system, making it easier for people to have their information removed, you know a number of MPs have raised concerns for constituents; also, to have information removed from the police national computer when it is not necessary, and on the other hand I suppose in

the case of investigations where there is the finger of suspicion pointed at communities and neighbourhoods for people to put their DNA on there for the purpose of elimination from inquiries. Is there a case for reforming the structure of the current system?

Mr McNulty: I certainly have no objection to the latter point, and would say that the more and more people who are on the DNA database in a voluntary capacity the better, just in general principally for exclusion. Once we have gone through the PACE review and the architecture surrounding the DNA database in that regard hopefully that will do what you seek in terms of de-bureaucratisation. If we are coming up with a much clearer retention policy, a much clearer criteria for retention, and a much clearer process for the general public should they want to come off the database and to at least have that avenue explored, I think that would be better all round and go to supporting the integrity of the DNA database.

Q500 Ms Buck: If the presumption of innocence remains a concern of the judicial system, and given also the significant disproportionality at every level in the criminal justice system on ethnicity grounds, how can the compulsory retention of DNA by people who are arrested but not subsequently charged be justified?

Mr McNulty: Because the DNA database is not a database of the guilty; it is purely an informational and investigatory tool for the authorities. There is no assumption of guilt because someone's sample is on the database. On the wider point about disproportionality, I take that point, but if the DNA database is the sum of all those who have encountered the criminal justice system and there are profound disproportionalities in that criminal justice system, then that is merely going to be reflected in the database. I do take that point very seriously, and we are working with the Attorney General and the Ministry of Justice to deal with that wider point about the criminal justice system.

Q501 Ms Buck: Why, therefore, if what you are saying is right, can people who are arrested but not subsequently charged simply be asked to volunteer to keep their database on the system and allowed not to if they so wish?

Mr McNulty: That may well be the way we go. I know the Chief Constable, Tony Lake, was very serious, as am I, in looking at the whole issue of criteria, retention, age limits and all the other assorted criteria. I think those are very fair points. When I say, like the NPIA, that we are roughly in a reasonable place in public policy and civil liberty terms given the nature of the database, I do not mean that is cast in stone, and we will look at retention criteria and other matters very seriously, but I do not accept the starting premise that somehow this informational and investigatory tool is counter civil liberties because it is not a database that is about the guilty, or, in the State's terms, the potentially guilty, that is why they are on. That is not the case at all.

Q502 Chairman: There are contingency plans, are there, for a massive leak of data off the DNA database in case this ever happens? You have plans in place?

Mr McNulty: As far as I am aware there are plans for such a contingency in terms of databases generally, yes.

Q503 Tom Brake: Minister, could I ask you for your reaction to what Gary Pugh is alleged to have said in relation to putting primary school children who might go on to become criminals in later life on to the DNA database?

Mr McNulty: Let me say in the first instance, if I may, that I wish Chief Constable, Tony Lake, the outgoing ACPO forensics expert well; he did a tremendous job, and I look forward to working with Mr Pugh, but I do not accept what he said at all, and nor do ACPO, as far as I understand it. I do not think that should get in the way of Mr Pugh making a significant contribution as ACPO forensics head, but I do not accept that premise at all. We are then getting into the realms of the point I made earlier about the sort of potentially guilty or the future guilty, and I do not accept that at all.

Q504 Tom Brake: The response from the Chief Constable was not supportive of it but what Mr Neyroud did say was that he thought, for instance, that the DNA database could usefully be extended in relation to working with other European partners, for instance. Are there areas that you are already aware of where you would like to see the DNA database extended?

Mr McNulty: Without putting words into his mouth, Peter Neyroud was talking more about extending the work on DNA across the European Union rather than extending the database in the context of the European Union, and you will know that in forensics, like a range of other areas, very happily, we are cutting edge in the European context, and certainly in terms of serious crime and in terms of terrorism and other matters at the heavy end, the greater work there is across the European Union and beyond on DNA fingerprints and others through Europol and, internationally, Interpol, the better.

Q505 Tom Brake: So there is nothing currently that United Kingdom Government is thinking of in terms of extending the United Kingdom DNA database?

Mr McNulty: No, save for my point earlier about there being a discussion around whether it should move to non-recordable as well as recordable crimes, an area I do not favour, and we are likely to come out against if I have my way. Beyond that, not.

Q506 Tom Brake: Moving on to CCTV, certainly in the public perception CCTV is effective at dealing with crime and assisting criminal investigations. Is that the Government's view, and is there evidence to support this?

Mr McNulty: I think it is broadly the Government's view. Firstly, it can act as a positive in the sense that the more people think their safety is enhanced by CCTV and others, the more people go out into public streets and spaces and, almost by definition, because there are more people about, there is a greater degree of safety in a sort of virtual circle. Can I point to a definitive national study that quantifies in any way its success as a deterrent? No, I cannot, but I am sure everyone can come up with significant local and anecdotal evidence to suggest that, as part of an array of other measures, it is successful, not just as a deterrent, not just in terms of bringing public spaces back into public use but also, crucially, as an investigatory tool for the police.

Q507 Tom Brake: There have been proposals for bulk sharing of ANPR (Automatic Number Plate Recognition) data. Do you think that will assist crime investigation and crime prevention?
Mr McNulty: I think it will, and it has. They remain proposals nationally but in the London context that is happening through a certificate of exemption granted under Section 28 of the Data Protection Action 1998 to be reviewed between Transport and the Home Office after a year, but both in the London context and in the wider context ANPR has proved very useful, not least in terms of serious crime and some particular terrorist cases, and I would like to get to a stage where the law is in a far more settled position than it is now. You will know that much of the ANPR cameras in the country were put up by the Highways Agency specifically for motoring purposes, so therefore, short of the execution of an investigation on a particular crime, not accessible to the police, and I would like that option to at least be restored so that certainly on our major motorway network and elsewhere there can at least be the choice of whether the police should be able to utilise ANPR from whatever camera.

Q508 Tom Brake: Do you think that TfL were right in expressing concern that handing over that data to the Metropolitan Police might lead to people taking action because of loss of privacy?
Mr McNulty: No, I do not. They were right to be concerned about getting the regulatory framework, the accountability channels and all the other elements that are essential to the use of such data in place, and that is a concern that I share, but, again, we are not talking about live ANPR feed that goes into some little room with the Metropolitan Police watching every single Londoner or visitor to London in their car at their choice and tagging them round on a nosey basis. It is done on a very focused, very specific, very intelligence-based fashion; more often than not the data is looked at speedily and destroyed. It is not about spying on people: it is about looking for, searching for, those who would do harm.

Q509 Tom Brake: So people who have concerns about CCTV, ANPR, integration of that data and so on have no cause for concern? We do not need to worry about our privacy?
Mr McNulty: I think they are fundamentally wrong in this regard because they talk about the entire network of ANPR and CCTV cameras as though they were all, as I say, on live feed, utterly manipulatable to the point of following someone from John o' Groats to Lands End when that is simply not the case. In any street you go down at least half the cameras or more will be private rather than public anyway, and many of those in the public domain will be on a very short feed, and the notion that they are just storing up all of this data at the end of the day, shipping it off to MI5, the police or anything else is profoundly wrong and not the case. Were that the reality then I would share some of the concerns of those who talk about a surveillance State , but it is not, so I do not. But at the other end, as I said right at the start, data protection, the rules and regulations surrounding what we do and how we do it with all aspects of surveillance as well as data, is uppermost in the Government's mind and, when that balance is right, I do say I think the critics are wrong.

Q510 Chairman: But, Minister, the demands of residents, and you must have this as a constituency MP, are insatiable in respect of cameras.
Mr McNulty: They would have CCTV cameras on every corner, but it is a matter of powers.

Q511 Chairman: Except on Brockley Hill?
Mr McNulty: Especially on Brockley Hill, I would say, on the Barnet side!

Q512 Tom Brake: Minister, you have highlighted that there is perhaps a misunderstanding amongst the public about how these operate, and in fact perhaps people's expectations of CCTV and ANPR are much greater in terms of what they can deliver than is really the case. Do you think there is an issue for the Home Office or perhaps for local government in terms of managing people's expectations about what realistically can be achieved in terms of tackling crime through the use of CCTV and other similar technology?
Mr McNulty: That is fair but my only caveat would be that no one in local government or central government, the Home Office, has ever suggested that CCTV of itself and on its own will combat crime. It is a key instrument across a whole range of policies that will help in this regard.

Q513 Gwyn Prosser: Minister, as you know, the United Kingdom is virtually alone amongst the common law countries of the world in allowing interception of e-mails and telephone calls and faxes and letters with the authority of a Government minister rather than a judge. Why do you think we are out of kilter with the rest of the world in this respect?
Mr McNulty: I suppose flippantly I could say they are all out of kilter with us, but we have gone for a statutory framework, a regulatory framework around commissioners and the law, that I think is appropriate and works. It is important too, as hopefully we will come on to, to distinguish between

interception per se and communications data. You quite rightly suggest that we can look at communications data in the fashion you suggest but communications data is not intercepted, and there has been a huge and wrong conflation of what powers are afforded under law to authorities on comms data compared to what there is in terms of interception, and I think it is an important distinction.

Q514 Gwyn Prosser: But in terms of this Committee's work on the surveillance society or the surveillance State, would you not say that the ordinary reasonable person in the street would be far more tolerant of allowing his or her data communications to be interfered with or intercepted or monitored if they knew that the authority for that monitoring was from an independent judge rather than a politician?

Mr McNulty: No. The question contains again part of the confusion. The Home Secretary, an independent politician, is not signing off the 253,557 requests for communications data that there were last year, and that figure is a matter of public record. That is separate from the 1333 interception warrants authorised by the Home Secretary from the 1 April to 31 December 2006. What the press have done over the last number of months is conflate the two and somehow suggest there have been over a quarter of a million interception warrants over the last year, which there have not been, and that there are some 700 odd authorities from local councils upwards who can all have a go and listen to your phone calls and get inside your e-mails at the drop of a hat. They have quite deliberately conflated the two, which are very distinct. Under RIPA there is a whole range of authorities who can and do have access to fulfil their statutory duties, duties that we as Parliament have put upon them, to do their job and look at people's communications data, ie look at who you have been phoning or e-mailing, et cetera, and no more. Just the traffic; not the content. When it comes to the content that is when the interception warrants prevail and that is the job of the Home Secretary to sign off. I think the way it is now, in terms of it being clearly embedded in the law and the legal process, with appropriate safeguards and oversight by an array of commissioners who authorise before certain processes can take part, is about the right place to be, but it is important to distinguish those two crucial elements. You will have all seen press coverage saying seven or eight hundred authorities all bugging your phone and looking at your e-mails and everything else, which is completely wrong—and quite rightly wrong.

Q515 Gwyn Prosser: In terms of the warranty interceptions, which we all agree are interceptions and intrusions, are you able to say why authority by a politician is better than authority by an independent judge?

Mr McNulty: It is not by a politician; it is by the Home Secretary.

Q516 Chairman: Is the Home Secretary not a politician?

Mr McNulty: Absolutely, but not any old politician; the highest politician in the land in terms of home affairs and these matters, and her job in that regard is again regulated and overseen by the Commissioners, and it is a power afforded to her by Parliament. Also, it is such a degree of intrusion I do not want it to be, in my own personal opinion, something that is a matter of legal norm by some judge. I would far rather it was that senior politician, and that she was held accountable for that.

Q517 Mrs Dean: Minister, could you clarify whether the Office of the Interception of Communications Minister oversees 795 organisations and, if so, does the Office have sufficient resource to inspect and oversee them?

Mr McNulty: They do. I do not doubt every office or agent of the Crown could do with more money but we have certainly not been told that it is creaking at the seams or whatever else because of lack of funding. The RIPA legislation is of itself very complex and very specific and very prescriptive, quite rightly, in terms of what people can do, how they can do it and what the frameworks are within which they can operate, and I think the oversight of that by the Commission is carried out and carried out very well. If the reviews that we are carrying out, as we said right at the start of the session, point out that that should be done in some other fashion or enhanced in some way then that is something the Government will look at, but I do not want to pre-empt the reviews or, indeed, the response of government to them.

Q518 Mrs Dean: In general terms, to what extent do you think the British public is aware of the wide powers granted by RIPA to permit access to communications data? Does it matter to you if people are wholly unaware of the general principles on which their behaviour can be monitored without their knowledge?

Mr McNulty: The more people are aware the better, and they can always be more aware than they are. In terms of the second point, again, if people are involved in entirely legitimate activities then they do not have to worry about RIPA at all, but some of the characterisations of the uses of RIPA as being "snooping" and "Nanny-statish" I do not accept. If someone with a significant track record for fly-tipping or whatever else in a local area persists and the local authority under its statutory duty wants to see if he has been phoning the fella on the other side of town who is in the middle of a construction site and no one knows where his rubbish is going, that is perfectly legitimate. Whether more people should know what RIPA entails and what activities it covers is a fair point, but they will not get that, frankly, from the sort of coverage there has been conflating comms data and interceptions, the way that has happened in recent weeks and months—which I entirely understand. It makes it a better story.

Q519 Chairman: Returning to the Rose Report and the Wilson doctrine, were you surprised to learn that there was surveillance equipment in prisons and that the conversations of prisoners were being listened into?
Mr McNulty: No, I did not find that a matter of surprise. The Rose Report was very comprehensive, and Sir Christopher Rose is to be congratulated for his speedy investigation. There was much concern that he had taken too long but it was done within a fortnight. The fact that there is surveillance in prisons I do not think should come as a surprise to anybody.

Q520 Chairman: So before the Rose Report you knew this was happening?
Mr McNulty: Not in the specific case, and nor should I, but the general principle that surveillance and intercept were part of a broad array of powers that the police service has —

Q521 Chairman: In prisons?
Mr McNulty: Yes.

Q522 Chairman: You knew this was happening in prisons?
Mr McNulty: I have knowledge that such things were happening in prisons as part of the general day-to-day work in prisons and the day-to-day work of the prison authorities along with the service and the police, yes.

Q523 Chairman: In respect of Members of Parliament and the Wilson doctrine, is it correct that no Member of Parliament has been under surveillance under the Wilson doctrine for four years?
Mr McNulty: The Wilson doctrine, as far as I understand it, firstly, is a matter for the Prime Minister rather than me. Secondly, in its historic origins at least, it was about phone interception and not much more, but as Rose says, as far as his study goes and it is the same to my knowledge, that is the case, yes, that no one has been under surveillance as a principal target by dint of being an MP. Sir Christopher clarified in his report that Wilson was not applicable in this case.

Q524 Chairman: But are you concerned that law enforcement authorities may gain access or information on, for example, who Members of Parliament may contact or the website used by MPs, either from Westminster or their homes? Is there any concern in your mind that some of this information might become available to agencies?
Mr McNulty: I do not think so because there is nothing in my mind that would lead me to think, as I have just answered, that it was going on or was about to go on in terms of MPs.

Q525 Chairman: Are there any lessons to be learned from the Rose report? Obviously you welcomed the report; it was set up by the Home Secretary and the Lord Chancellor; you have studied it carefully. Is there anything that could be learned from the experience of what happened, because it did cause excitement.
Mr McNulty: It caused plenty of excitement, certainly, and the Home Secretary said at the end of her statement that we will look at, in the light of the Rose report, all the assorted statutory codes of practice that prevail around the whole issue of surveillance and intercept, not least in the context of Wilson, and that we should get to a stage where confidential discussions between an MP and his or her constituents in the broadest sense should be as sacrosanct as a legal discussion between an appointed legal representative and an individual.

Q526 Chairman: Has that review begun? We know that a review was announced by the Home Secretary, and she said she would get it done by the end of the year. Has the process started?
Mr McNulty: The scoping of the process has started. It is potentially either, if you think about it, a very narrow piece of work or a very broad piece of work, and I think the broader the piece of work and the better done it is, the better—and I apologise for that, but in part it will go to the outcome of a range of the reviews we are doing that we referred to at the start, so it is alongside those processes.

Q527 Chairman: Indeed. It just sounds a little bit vague to me and you are very precise, normally, as a minister; you give us straightforward answers. Has the scope of the review been agreed? Because it is a very short timetable until the end of December, is it not?
Mr McNulty: It is and, as I understand it, and I will stand corrected, I said quite precisely that the scoping of the review has begun. Quite what the full scope of it is and the terms of it —

Q528 Chairman: And who is doing it?
Mr McNulty: It is happening in the Home Office.

Q529 Chairman: And do ministers have responsibility? Is it your responsibility?
Mr McNulty: Ultimately it will be the Home Secretary's responsibility.

Q530 Chairman: So the scoping process has begun?
Mr McNulty: As far as I am aware, yes.

Q531 Chairman: Are we on timetable to complete this by the end of December?
Mr McNulty: I would say so, short of anything coming out of the broader reviews on data that I alluded to at the start of the process.

Q532 Mr Clappison: What are the arrangements for telling Parliament about what is happening?
Mr McNulty: As and when there is something to tell Parliament, Parliament will be told. The Home Secretary has undertaken to report back to Parliament in terms of whether or not the current codes of practice clarify, I think she says quite deliberately, the extent to which reviewing officers and authorising officers should pay special attention

to conversations involving or potentially involving a Member of Parliament, and I am surely Parliament will be told in the normal fashion. The Codes will be available for Public Consultation later in the year. All the RIPA Codes are subject to the affirmative process so any changes will need to be agreed by both Houses.

Q533 Chairman: I think it would be helpful if we had a note on this from the Home Office because it does sound a little bit vague to me.
Mr McNulty: I do apologise if it sounds vague but it does go alongside our review of the codes more generally in terms of what I was saying earlier, but I will happily do a note on where we are at with the timelines for all those codes, where we are—if I can, because we do not control all of them—in terms of the broader reviews I outlined at the beginning, and where this specific one fits in, and in what fashion, as Mr Clappison says, Parliament will be informed at the end of the process—probably, as the Home Secretary indicated, by the end of the year.

Q534 Chairman: Could we have that note by the start of the next session? In other words, by 18 April?
Mr McNulty: I should think so, yes.
Chairman: Thank you very much.

Q535 Ms Buck: Turning to identity cards, remind the Committee, in the regulatory impact assessment of the Bill was there a specific assessment of the contribution that cards would make to the particular strands that have been flagged up as significant? The immigration, the e-terrorism?
Mr McNulty: Specifically on each of those? I do not think so. I think it was a broad general regulatory impact assessment that normally goes alongside these pieces of legislation.

Q536 Ms Buck: Have you made assessments of that kind? In the Home Office, is there an assessment of what would be likely over, say, the course of ten years?
Mr McNulty: There have been broad policy assessments. You will know that the *National Identity Scheme Delivery Plan 2008* has come out since Meg Hillier met the Committee to talk specifically about ID cards. Has there been a quantitative and empirical study of the benefits of ID cards specifically in the context of e-crime, cyber crime, terrorism, and illegal immigration? Not in that specific sense, no, because we are not futurologists.

Q537 Ms Buck: No, but surely --
Mr McNulty: Has there been substantive work done on the public policy dimensions associated with the benefits that were outlined in the original Bill and the original regulatory impact assessment? Yes. Are they detailed quantitative pieces of work? No, and I do not think that is extraordinary.

Q538 Ms Buck: No, but, on the other hand, if one is being asked to make a very substantial investment of public money in areas like terrorism it must be very hard to make that investment, but in areas like immigration and e-crime I would imagine it might have been possible to make an assessment of the cost benefit?
Mr McNulty: It is easier but it is still very difficult, not least because the Committee will know that on the identity theft side there are enormous innovations all the time as well, and almost as you come to such assessment the rules change in terms of what criminals do. As far as possible there is in public policy terms and more generally an assessment. I do not think I have seen any detailed, quantitative, mathematically sound piece of work done on the public policy consequences of a significant piece of legislation, certainly in the last ten years or, in studying politics, over the last thirty years.

Q539 Ms Buck: But on the issue of identity crime is not the whole point that the identity card is being put forward as a kind of Gold standard that would effectively mean that whatever criminals did to try and catch up, a DNA-based ID card, biometric ID card system would keep you —
Mr McNulty: Database.

Q540 Ms Buck: Biometric, sorry.
Mr McNulty: Yes, and those assessments have been done. If you are asking for the quintessential, comprehensive, all-singing, all-dancing, quantitatively, mathematically robust, cost-benefit analysis, no, it has not been done.

Q541 Ms Buck: No, I was not. I was asking for anything.
Mr McNulty: Well, there has been, and they have been released over the course of time. When I took the Bill through three years ago there was significant cost-benefit analysis work put into the public domain around some of those aspects. As you quite fairly say, it is more difficult in other regards.

Q542 Ms Buck: The Sir James Crosby report put a lot of emphasis on the consumer-led benefit of identity cards and the belief that by promoting to the citizen that benefit entitlement, entitlement generally, it would be much more effective really in the crime-fighting side of the benefit of the card because it would be winning public confidence. You have been very strong in articulating the entitlement card benefit aspect of it. Why did the Government not do more of that?
Mr McNulty: The Government has done more and more. Without drifting into a rather boring anecdote, I had a very nice holiday in France spoilt by journalists getting in touch with me about my latest musings on ID cards when I was responsible for them in the middle of August, with a front page splash on *the Guardian* and Lord knows what else, because I had done a Fabian seminar about four or five weeks before where I said that it was difficult to sell or get over the strength of what I think was such a profound piece of public policy if all you are saying is: "Thanks very much, here is what it does for the State, it is nothing to do with you", whereas ID

management and control is getting more and more important for the private sector as well as the public sector. Everyone knows that more and more applications revolving around someone's identity will be utilised by the private sector, so the more and more we can say, I think quite fairly, that there is a range of transactions that each individual will take in the future that will be better helped and better secured through the utilisation of ID cards, the better. That is not to reduce the benefits to the State; I think they are still there, but it is not just about what an ID card imposed on people or otherwise can do for us, the State. It really is about what it can do for the individuals, and getting that balance right does mean that the popularity of ID cards will be even more than it is.

Q543 Mr Winnick: Do you understand the concern, Minister, which is felt and felt pretty strongly, that the introduction of ID cards and particularly the Identity National Register is a threat to civil liberties?
Mr McNulty: I understand it; I do not agree with it.

Q544 Mr Winnick: There is a view that the concern which I just mentioned is just held by *Guardian*-reading wimps, and really is totally unjustified. That is more or less your view.
Mr McNulty: I do not agree with that characterisation of those who hold the view that ID cards are somehow antithetical to civil liberties, but nonetheless I still disagree with the premise that it is antithetical to civil liberties.

Q545 Mr Winnick: Does it surprise you that, rather like in Australia, opinion polls, for what they are worth, showed in the beginning quite strong substantial support for ID cards but that seems to have declined, and I am talking about ID cards for UK citizens and residents. Does that in any way surprise you?
Mr McNulty: It has declined, but the last time I saw any notion of public support it was still quite significant. It was not quite the high 70s or so as I think it was when this was talked about the first time the Bill was put through but then ran into the 2005 Election, and then I picked the Bill up afterwards; nonetheless I still think there is a significant degree of popularity and support for ID cards, but that is not the principal reason, I hasten to add, for pushing the piece of public policy through.

Q546 Mr Winnick: I have seen opinion polls, as I say, that show a marked decline, but we will wait and see what happens with the next one. Is it intended to publish a full privacy impact assessment of a National Identity Scheme?
Mr McNulty: Not in the sense that the Bill is secured, so anything that will go alongside a piece of legislation, like your regulatory impact assessment and other assessments, where the Bill is now some two or three years old. I would say, though, as made clear in the Bill at the time, any subsequent move to a compulsory registration on the identity database would be the subject of further primary legislation, and it may well be then that the broader impact, including privacy, would need to be looked at.

Q547 Mr Winnick: It is quite a serious issue, is it not?
Mr McNulty: Very serious.

Q548 Mr Winnick: Professor Ross Anderson, a professor of security engineering at Cambridge University who has often given evidence to us, gave evidence more recently to the United Kingdom Borders Bill Committee about the possibility of biometric data being stolen, and was rather pessimistic about that. What contingency plans have been made in the event of that happening?
Mr McNulty: In a sense I would turn that round. The National Identity Registration Scheme database is, by definition, being brought in in very incremental fashion, so both the security of it and the efficacy of the IT software access and all the other elements, will be learned and relearned on an evaluative curve and feedback loop at each stage. We have quite deliberately eschewed the notion—not least I would guess in passing because the most lamentable of government IT projects are those that are Big Bang and you switch from one system to another straight away and not least because of the importance of security and other aspects—of going full on for introducing things in one big hit, so there will be incremental lessons learned on security, on access, on the architecture and on the efficacy at every stage of the implementation of the programme as identified in the *National Identity Scheme Delivery Plan 2008* that I think came out, as I say, just after Meg Hillier had been before the Committee.

Q549 Patrick Mercer: Minister, thank you for your replies so far. Given the lucrative nature of much e-crime that we see and its damaging effect on the private individual, are you satisfied that the current penalties for these crimes are adequate?
Mr McNulty: I suspect I am not, and I suspect that one of the compelling points that Government needs to get to grips with in the future is the whole nature, in the first place, of e-crime, cyber crime and those other dimensions, and then revisit the whole legal framework and sanctions on such crime. I think it is an area that collectively, at ACPO, the services and more generally, we need to devote a lot more time and effort to, and at the back end of that process I would say that these sanctions and punishments for such crimes may well need to be looked at as well.

Q550 Patrick Mercer: Do you think organisations that compromise personal data ought to be made to pay compensation?
Mr McNulty: I am no expert in the matter but I think that may be something that should be looked at.
Patrick Mercer: Thank you very much.

Q551 Mrs Cryer: Minister, can I ask you a couple of questions about growing trends? The first one is the growth of social networking sites and what impact this is having on the fight against crime.

Mr McNulty: That is a very interesting point and I am not sure that collectively in the United Kingdom or elsewhere we fully understand the ramifications. There are certainly hints, and probably no more than hints at the moment, that there are people fishing—I can say that now Mr Salter has gone!—through *Facebook* and other social networking to elicit personal information that will go to potentially identity theft, and I think people need to be very wary, not of the interaction that comes from *Facebook* and other such social networking sites but what they put on there, what goes into a public domain and what can be potentially lifted off by miscreants for the wrong reasons. It is an area that collectively we need to keep under review. I am on *Facebook* and it has not done me any harm yet—as far as I know!

Q552 Mrs Cryer: Do you accept there is greater surveillance now than ever before, and do you believe that arguments for individual privacy are overstated in relation to public protection?
Mr McNulty: I would probably say "No" to both of those, if that is not contradictory, in the sense that in the very narrowly defined sense of State surveillance and intrusion into people's lives, I do not think it is significantly more troublesome than it was in the past, not least because I think the regulatory and the statutory framework that governs it is all the more robust now than it was before. There are still, regardless of what I say about the databases, surveillance and everything else that we use, still profound issues around privacy, civil liberties and data protection, and it is our job to get that balance right. So I am not pooh-poohing the notion that there are not civil liberty concerns; I am saying that thus far, and with the reviews and we will see if we need to amend them in any way, we have the balance about right between the regulatory framework, the statutory route of these things, and the concerns around privacy and civil liberties. It is just that some of the real areas of concern and worry are blown up to this Orwellian picture of Big Brother or Big Sister looking over everybody's shoulder, which makes great copy but is miles away from reality.

Q553 Chairman: Following on from what Mrs Cryer has just said, in today's *Independent* there is an article about Tim Berners-Lee, the inventor of the World Wide Web, who warns about --
Mr McNulty: I thought Al Gore invented the World Wide Web!

Q554 Chairman: I do not know who invented it but he is claiming to do so, and he says we should be very wary of new technology being contested by three British internet suppliers, one a company called Form, who are able to track the websites of individuals, and he has met Government ministers and expressed his concern to them. You may or may not have met him, but this is a concern, is it not, that the internet is now being monitored in this way?
Mr McNulty: To go back to Mrs Cryer's point and the point about trends, there is a general concern that we need to keep apace as Government—and individuals, by the by—with the adoption of apparently benign technology; that with every significant quantum leap in the application of technology for good there are those who would use it for ill and negative purposes, and collectively and certainly as Government we need to keep apace of that. I fully accept that.

Q555 Chairman: What would you say to the teachers' leaders and their General Secretary, Mary Bousted, who says that cameras being installed in schools may well be used to monitor teachers?
Mr McNulty: I would say, from the little I know of the project, that it is profoundly wrong of her to suggest that and, as far as I am aware from colleagues, cameras put in schools are there principally for the protection of teachers and pupils alike. Again, in terms of this notion of myth, there is not a feed back into the local education authority just to have a look at what this teacher or that teacher is doing, and by perpetuating, or seeking to help perpetuate, that myth she does not do herself or the profession great credit.

Q556 Chairman: And you are quite confident that we do not now live in a surveillance society? You seem to be putting much of the blame on the press for using information in order to puff up the concern.
Mr McNulty: With respect, I do not blame the press or media; I do not really indulge politicians who say it is all the media's fault, I think that is nonsense. What I do say, and I said this at the beginning, is that fears that people have over a surveillance society form much of the meat of myths rather than reality. Also, given that we have, quite rightly, collectively as Parliament and certainly as Government, real concern about the regulatory oversight, data protection and other statutory elements that make us get the balance about right, any concerns about George Orwell being round the corner in terms of 1984 are much exaggerated, but we should remain ever vigilant.

Q557 Chairman: You are the Counter-terrorism Minister, and we are looking at the terrorist implications for all this and have examined the Counter-terrorism Bill. Do you have information for us as to when the Second Reading of the new Counter-terrorism Bill is coming before the House?
Mr McNulty: I will leave that to the Leader of the House on Thursday, if I may.

Q558 Chairman: Is that a hint that something will happen on Thursday?
Mr McNulty: No, just a hint that the Leader of the House determines the time and the business rather than my good self.

Q559 Patrick Mercer: Minister, in the same capacity, have you any insight into when the Government might be announcing its national

security strategy?

Mr McNulty: As many of the very informed gentlemen and ladies of the press have suggested, maybe on the morrow.

Chairman: We will go now into private session to meet Congressmen Steve King and Congressmen Louis Gohmert from the US Congress, but can I thank you, Minister, very much.

Written evidence

APPENDIX 1

Memorandum submitted by Brian Leapman

I am Brian Leapman and I was the author of the Diamond vision paper produced by SITPRO Business Process Analysis Working Group that was used to get the various UK Ministries to sign up to the concept of joined up government and the Single Window concept. I am presently involved in a project to build an Interoperability Service Utility ISU that will provide interoperability and collaboration capability across multiple organisations, businesses and regulators seamlessly for the cost of a phone call that we are attempting to get EU funding for The EU commission has made this one of their infrastructure priorities for the development of the EU.

An ISU will be able to take feeds of structured and unstructured information from databases, applications, emails, conversations and videos and deliver the information to the user in a search engine capability. The media and content makes no difference to the comprehension of the information as relational semantic is used that is language independent.

In our application for funding we have highlighted an important social issue:

— At one level the ISU is a great tool in that it provides a customised view of the world to the needs of the individual or organisation. This is called the Multi Single Window MSW.

— At the same time it gives the possibility as a result of seamless interoperability the possibility of government being able to obtain the Single Multi Window SMW the omni view. This is the BIG BROTHER fear that society quite rightly is concerned about.

Technically, we cannot create the MSW without the possibility of creating the SMW and whilst the first is desirable the second outcome is not so desirable particularly if the power is abused.

The issue around the SMW is not that it can occur:

— But under what circumstances?

— What are the controls on that power?

— How do we make sure that the power is not abused?

Technology it should be remembered is neutral. IT IS THE USERS WHO ARE EITHER BENEFICIAL OR MALEVOLANT TO SOCIETY whether the terrorist, the individual, business or government.

Some of the risk can be mitigated through the instigation and provision of Role Access User Digest provision of information. We are building this into the architecture of our ISU. In very simple terms the enquiring user, which could be the government, can get the salient information without access to information that is not regarded as relevant or that is personal to the individual or organisation. I call it the Reader's Digest version you get all the salient information without having to waylay through the whole story.

For instance, let us say that the police want to know if someone had been in hospital on a set of dates. If we expose the full medical record; they would have private information that really the police have no use for or need for, and that an individual officer could use improperly. However, in the Role Access User Digest model, the police information receives a reduced report from the medical record that shows only the dates and time of entry and exit. Let us say there was some relationship between the entry into hospital and a particular crime. That search request would be sent to the hospital, the police would be denied entry to the search until the hospital had satisfied itself of the necessity to reveal the additional information.

Whilst this may not be the actual scenario, I hope I have illustrated the way well designed process management can be used within the technology to mitigate the risks of the abuse of the Multi Single Window.

In my opinion, there will be an increasing need for a standing body, somewhat like the Audit Commission, made up of professional business and technical process architects, security experts with an element of legal council that has the power to independently investigate abuses of government intrusion and liberty, with the right to independently audit government departments and agencies and to provide recommendations of functional improvement.

The issue of government and the wider society battling over intrusion towards a surveillance society is going to be a continual ongoing concern for all parties. At the same time government is charged with the creation of a more interoperable collaborative and visible open society. They are in essence two sides of the same coin. Our suggestion is the creation of an independent entity charged to maintain the benefits with as little compromise as is technically possible to the freedom of the individual and organisations.

March 2007

APPENDIX 2

Memorandum submitted by Mr William Selka

Firstly, congratulations in identifying this issue as important.

Privacy and rights (or absence of them) of the individual have long been a differentiating factor between the UK and other countries and I believe are an essential ingredient of "Britishness".

Personally, I don't mind the state knowing where I am, but I do object to the state having the right to know.

The ability of the courts to apply common sense and the layers of overlapping laws and precedent gives the UK the best and fairest legal systems in the world. I am a big fan of the idea that you can do anything that isn't illegal, rather than having to have permission for everything.

My concern about the drift of the state towards surveillance, in particular ID cards, is that it potentially changes the legal definition of an individual from something that the courts assess at the time of the charge to a set of attributes on a computer. I refer to the courts because this is where a disagreement between the individual and the state will end up. ID cards may be cheaper to administer than the current system of identification in court but there are huge opportunities for abuse. A set of attributes on a computer can be sold, modified and duplicated in a way that the individual themselves cannot be. I am not even sure whether the ID card scheme will be cheaper to administer, as the expected costs look horrific.

If the state redefines the relationship with the individual as a relationship to this computer data, this will significantly undermine for me the attraction of being British, taking a step backwards, becoming more like other countries in the world.

You may be able to quote existing miscarriages of justice and administrative difficulties as justification for increased state surveillance, but to give up on the principle for practical reasons would be profoundly sad and an indication that the government does not appreciate the jewel that the UK currently has, in the strange way that the relationship between state and individual has developed.

I have never made a submission to a committee before, so I am not sure whether this is in the correct format, but please do not underestimate the importance of your work and please, please, don't let us sleepwalk into a situation where the identity thieves get more power and individuals less freedom due to the state's administrative laziness and desire to control its subjects.

As a minimum, if the worst happens, and the government and computer industry is successful in forcing ID cards onto us, I would like to see penalties for civil servants who sell identities to be extremely severe, on a par with treason.

April 2007

APPENDIX 3

Memorandum submitted by Dr C N M Pounder

1. Recommendations

The evidence in my submission leads me to invite the Committee:

— To conclude that the use of surveillance technology in a post 9/11 age raises the question of whether there should be an explicit right to privacy.[1] Such a right would raise issues which are broader than the surveillance state. I would also recommend that an independent inquiry should explore whether or not the law should be augmented with this right.[2] The form of this inquiry, its members and its terms of reference must stress independence from Government, as Government has a vested interest in its outcome.

[1] The Culture, Sport and Media Select Committee (session 2002–03; HC 458, "Privacy and Media Intrusion") recommended that Parliament should bite this particular bullet—otherwise the Courts will develop the law in this area—a prediction which is coming true. The problem is that cases before the Courts usually involve the media and celebrities with the result that case-law can become unrepresentative of the privacy issues faced by most of the population. (My own view is published in Home Affairs Committee, Fourth Report, "Identity Cards", Session 2003–04, Volume II (Ev 281–283).

[2] My own view is that a right to privacy, enforceable via the Sixth Data Protection Principle, would buttress the position of data subjects and by keeping it within the framework of the Data Protection Act would not disturb the issues which relate to the Press.

— To state that the processing of personal data via new technologies, or the processing of personal data that are subject to data sharing and data retention polices should be subject to a strengthened data protection regime where procedures which protect individual privacy can be independently established, monitored, reviewed and enforced.[3]

— To augment the recommendation from the Joint Committee of Human Rights (JCHR)[4] with respect to the production of a Human Rights Memorandum/Assessment and state that any Privacy Impact Assessment be incorporated into the JCHR recommendation. The joint Human Rights/Privacy Impact Assessment should be published as part of the Regulatory Impact Assessment for any Bill. Such Assessments should also be post-dated for Acts of Parliament which impact on privacy (e.g. Civil Contingencies, anti-terrorism, Children Act, ID Card Act and Criminal Justice Acts).

— To recommend that there should be fewer Commissioners involved in the privacy protection business, and in the case of national security, a mechanism should be developed whereby operational matters can be assessed.[5]

— To call for a review of Parliamentary procedures in order to identify the lessons that should be drawn from the lack of scrutiny which has occurred with the decision to use the National Identity Register as a population register. If the Committee find the evidence on the Annex compelling, I would ask the Committee to recommend the use of Parliamentary procedures so that section 1(4)(e) of the ID Card Act 2006 becomes inoperable.[6]

2. Why Privacy is at Risk?

In general, the current framework of the law and as it impacts on privacy (ie the Human Rights Act; Data Protection Act) does not protect privacy to the extent imagined. I have detailed these arguments elsewhere[7] but I summarise the main points below.

1. Government Departments are increasingly being considered to be a single data controller whereas the Data Protection Act assumes an array of separate data controllers. This change is a consequence of data sharing statutory gateways which 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).

2. 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 degrades the protection afforded by the most Principles.[8] So when Ministers claim that "the Data Protection Act applies" the claim can be disingenuous,[9] if Ministers can subsequently use powers to modify the impact of the Principles.

3. Legislative powers which impact on the processing of personal data are often needed to provide flexibility as to how the processing of personal data is to occur, or to allow for the use of the techniques or technology not yet designed. A problem arises because the time when the legislation is enacted by Parliament is often separated, by years, from the time when policy is implemented through the use of technology. To introduce a degree of flexibility, widely drawn powers are defined and this exacerbates the risk of function creep or use of powers by a future Government in a different context. The Identity Card project is an example of how aspirations for the use of a database can change.

[3] There are several possibilities that can introduce independence. For example, Codes of Practice dealing with personal data could need to be approved by the Information Commissioner before they can come into effect rather than a commitment to "consult" the Commissioner. The Commissioner could have the power to require Parliament to review the operation of Ministerial power, if need be. The Commissioner could possess the ability to ask the Court, in certain circumstances, to strike out Statutory Instruments. The Commissioner could have powers of entry to assess compliance with provisions a Code of Practice. Identifying these independent mechanisms should be part of the inquiry refereed to in the first recommendation.

[4] 19th Report of the Joint Committee on Human Rights (session 2004–05) calls for a "Human Rights Assessment" to be published.

[5] I estimate there are at least seven Commissioners who work in the privacy arena—see footnote 14.

[6] The decision to use the NIR as a population register arguably reproduces all the problems that Parliament had in scrutinising the "War in Iraq". If this is the case, it can be argued that if the public administration purpose is to be subject to these problems, then they are likely to be endemic in the way Government makes any decision. It follows that Parliament has to look at strengthening its powers of scrutiny (eg a mechanism to demand any document from Government; Members of Select Committees to be able to cross examine Ministers and Civil Servants via the use of experts and/or leading counsel in the questioning; Members of Standing Committees on Bills to gain access to civil service briefings given to Ministers re member's amendments to legislation).

[7] Details in Home Affairs Committee, Fourth Report, *Identity Cards*, Session 2003–04, Volume II (Ev 169–73 and Ev 276–81).

[8] 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.

[9] 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.

4. Powers established by Parliament in a bygone age have been used to justify vast tracts of data sharing or data access.[10] It is 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).

5. Retention policies (eg DNA database, communications data, retention of ID Card data) enhance the surveillance potential of the data and raise questions of trust.[11] 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.

6. 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. In the Serious Crime Bill before Parliament, for example, the Audit Commission are similarly conflicted.[12] This conflict of interest has to be resolved: the organisation/Minister performing (or responsible for) the interference should not have control of the rules which protect privacy from that interference.

7. 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 (eg the processing is necessary for the delivery of *one* particular service—for example, Council Tax).[13]

8. 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.[14]

9. 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).[15]

10. 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.[16]

11. 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 (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.

12. 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 to 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.

---

[10] 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).

[11] 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 childrens details being retained on a child at risk register when there is no risk, and patients who object to the holding of medical records centrally.

[12] The Audit Commission is to produce its own Code of Practice to govern its own data matching activities.

[13] 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, there is no viable test as any data item X is likely to be relevant to the efficient delivery of public services. It is going to be difficult to show a breach of a Principle if the Commissioner has to prove "inefficiency". Most of the data protection principles are defined in terms of a purpose which is assumed to be narrow.

[14] 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.

[15] 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).

[16] Unlike the FSA which recently fined the Nationwide £1 million for breaches of security of personal data.

13. Data subjects and data controllers cannot contribute directly to the policy or procedures which surround data protection compliance. Ministers produce Codes of Practice in isolation from data subjects whose personal data are processed and data subjects are often excluded from the process of producing a Code of Practice.[17]

14. Parliamentary scrutiny of privacy matters needs to be strengthened, especially when powers which impact on privacy are used by Ministers. The European Parliament has little power in respect of decisions made at the Council of Ministers. This is especially the case in the field of national security.[18]

15. The current Parliamentary arrangements are not responsive to the increasing number of international commitments, unofficial agreements between Ministers from different regimes, and treaties which require transfers of personal data from the UK to other countries.[19]

16. Parliament does not receive the information it needs to scrutinise legislation in the field of Human Rights.[20]

17. The current arrangements do not contain a viable mechanism which emphasises the complimentary nature of data protection and law enforcement, and which can ease the tensions which arise. Maintaining the privacy of the individual and assisting the authorities in the field of law enforcement are far too often seen as in total opposition, when in most cases, they are complimentary (eg security of disclosure of personal data; accuracy of data disclosed).[21] However, 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.

3. Scrutiny of the Use of Powers is Inadequate

Parliament grants Ministers wide powers mainly because Ministers claim that a degree of flexibility is needed to face a specific threat. This accounts for the generous enabling powers found in legislation such as the ID Card Act, the Civil Contingencies Act, the Children Act and most anti-terrorism legislation. So the question arises as to what is the counter-balance to misuse of these powers?

Ministers correctly claim that if the detailed implementation of their powers by Statutory Instrument (SI) breaches the Human Rights Convention, then these SIs could be struck out by the Courts using its powers under the Human Rights Act. This position is then developed to argue that 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*. This approach is illustrated by the letter the Home Secretary wrote to the Joint Committee on Human Rights in relation to the ID Card scheme (JCHR's 8th report):[22]

> ". . . Secondly, I must stress that the Identity Cards Bill is *enabling* legislation. Many of the precise details relating to the application process, the format of the ID card itself and the arrangements for the provision of information from the National Identity Register have yet to be decided. We have therefore not spelt out all the details on the face of the Bill and many of these can only be set out later in secondary legislation which will also have to be compatible with our ECHR obligations. 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. *We will be under a duty, under section 6 of the Human Rights Act, to act compatibly in making the subordinate legislation and if we did not do so the courts will have the power to strike it down*".(my emphasis but Home Secretary's emphasis on *enabling*).

There are several problems raised by this approach:

- Government can use the "powers could be struck-out" argument to ignore any criticism in Select Committee Reports which relate to wide ranging powers.[23]
- scrutiny of primary legislation by Parliament when granting the powers can be limited because of the timetabling procedures can be used by Government to stifle debate on important topics.

---

[17] 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.

[18] Joint Committee On Human Rights, Third Report ("Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters"), Session 2005–06, Written Evidence 156.

[19] International Treaties or Decisions of the Council of Ministers are often presented to Parliament as *fait accompli*—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.

[20] 19th Report of the Joint Committee on Human Rights (session 2004–05) calls for a "Human Rights Assessment" to be published.

[21] If staff are properly trained in procedure, if powers are properly applied in the correct way and in the correct circumstances, and there is no "mission creep" or "function creep", then privacy and security can co-exist.

[22] Joint Committee On Human Rights, 8th Report, Session 2004–05, Appendix 1.

[23] See recommendations 59 and 60 of the Committee's report into ID Cards Report where the powers were described as "unacceptable", yet they exist in the ID Card Act 2006 in the same form.

— the secondary legislation associated with the use of powers is not subject to line by line scrutiny or much debate—Ministers can exercise powers without adequate scrutiny or review.

— 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;[24] there are about 2,500 Statutory Instruments (SI) per year and, unless the SI is technically defective, most are not challenged.

— 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.

— 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.

— It is possible to envisage circumstances in which even where secondary legislation is struck out, Ministers would just draft another instrument circumventing any problem raised in Court. Therefore any legal challenge would need to start again at square one.[25]

The JCHR has already commented on the problems identified above. In its 19th Report[26] the JCHR stated that:

> 81. . . . we have noticed that the Government frequently employs two related catch-all defences to our compatibility queries. One of these defences is that wide discretions granted to public authorities by a bill do not raise compatibility questions because, under section 6 of the Human Rights Act, such authorities will be behaving unlawfully if they act in a manner incompatible with a Convention right. The second defence is that order- or regulation-making powers contained in a bill, however broad, do not present incompatibility risks, because such delegated legislation, unlike primary legislation, is normally invalid to the extent that it is incompatible with a Convention right. Both these defences go to the heart of the purpose of our scrutiny of bills for human rights compatibility, and the effectiveness of scrutiny, particularly in relation to bills which are essentially "enabling" legislation, such as the Identity Cards Bill of Session 2004–05. In our view, one of the most important features of the scrutiny we perform is that it is preventive in nature, aiming to minimise the likelihood of new legislation giving rise to breaches of human rights in practice. We consider this to be a constitutionally different function from the ex post intervention of courts when deciding whether a public authority has acted incompatibly with Convention rights.

This led to a recommendation from the JCHR (also in the 19th Report, session 2004–05), that Government should publish, with each Bill, a Human Rights Memorandum which will:

— "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 engaged;

— 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; and

— cite the evidence that has been taken into account by the Department in the course of its assessment."

[24] 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).

[25] 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).

[26] Session 2004–05, paragraph 81.

[27] 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".

The Government has not accepted the above recommendation,[27] however, such a Memorandum would chime with the Committee's consideration of Privacy Impact Assessments. 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.

4. Parliament has to Scrutinise Legislation Effectively

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.[28]

The evidence I now lay before the Committee (detailed in the Annex) concerns how plans to merge the Citizen Information Project (which dealt with general public administration) with the NIR (which dealt with security matters, immigration and law enforcement) were taken without effective scrutiny by Parliament and contrary to a promise of a further round of public consultation.

My own view is that the evidence also raises an important question for Parliament. 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?

In summary, the evidence in the Annex suggests:

- The Government cannot claim public support for the use of the NIR as a population register as the public consultation on the ID Card specifically *excluded* the use of the NIR for a general public administration purpose.[29]
- Because of the privacy implications of establishing a population register for a general public administration purpose, the Government, in its public consultation, promised a further public consultation as it was necessary "to explore the issues around public acceptability of the proposal".[30] This consultation has not taken place, yet the decision to transform the NIR into a population register was taken when the ID Card Bill was before Parliament.
- The Government's responses to several Parliamentary Committees (eg to the Home Affairs Select Committee in October 2004) do not fully reflect the decisions which were taken to use of the NIR for a general public administration purpose.
- The Home Secretary was informed in September 2004 (months before the First Reading of the ID Card Bill in June 2005), that the use of the NIR for a general public administration purpose would require a compulsory ID Card.[31] This important justification for a compulsory ID Card has not featured prominently, if at all, in any public debate, nor in any Government document, and nor in any Ministerial statement to Parliament (eg during the passage of the ID Card Bill).
- The opportunity to identify the use of the NIR for a general public administration purpose did not feature in Labour's Manifesto for the General Election. The Government cannot claim that this part of the ID Card's implementation has public approval by virtue of an electoral mandate.
- Officials knew before the General Election of 2005, that the use of the NIR for a general public administration purpose represented 20% of the business case for the ID Card scheme. Yet this and other facts were omitted from the ID Card Bill's Regulatory Impact Assessment laid before Parliament.
- Around the time of the First Reading of the ID Card Bill in June 2005,[32] 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.

---

[27] 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".

[28] Q782, Fourth Report of Home Affairs Committee, Identity Cards, Session 2003–04, Volume II.

[29] The public consultations (CM 5557 and CM 6178) both gave commitments to use the ID Card and related NIR for limit purposes (eg to crime and security issues).

[30] Paragraph 3.20 of CM 6178 ("Legislation on Identity Cards").

[31] Citizen Information Project: CIP progress report—10 September 2004 on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp.

[32] See Appendix 1 and the events of 30 June and 13 July 2005.

— There were 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.[33]

— Throughout the lifetime of the Citizen Information Project, senior officials from the ID Card project were in attendance, and the minutes indicate that Ministers were informed. However, it is possible that because of the change of Home Secretary in December 2004[34] combined with a breakdown in communications between civil servants and Ministers caused Parliamentary scrutiny of certain aspects of the ID Card scheme to be considerably weakened.

5. Data Sharing, Trust and Surveillance

The question about effective Parliamentary scrutiny can also be related to the issue of trust which underpins the debate about the surveillance society (and a functioning democracy). If Government cannot be trusted to submit to scrutiny (by Parliament or via public consultation) when the purpose is "public administration", why should the population trust its processing of personal data for other purposes?

My own view is that the main issue with data sharing is usually not *WHETHER* there should be data sharing, but rather *HOW* such data sharing is to occur. Taken from this perspective, there are only three policy options for such data sharing:

— The data subject is in control of the data sharing and consents to it.

— Data sharing occurs but the data subject can easily object to the sharing.

— Public bodies are in control of the data sharing. The data sharing is compulsory and sanctioned by statute (and where the data subject could object in the very limited circumstances of the Data Protection Act by showing that data sharing causes substantial unwarranted distress or substantial unwarranted damage).

What I suspect has happened, is that without debate or public consultation, the Government has shifted its policy. In the original PIU Report[35] on data sharing, for example, data sharing was only based on compulsion in the obvious cases (eg by providing a statutory gateway to allow the law enforcement agencies access to data, or to the emergency services in cases of public health issues). In all other circumstances, the PIU report recommended consent of the individual concerned to facilitate all other data sharing activities where compulsion was not justified by the obvious cases.

However, in April 2003, the Government obtained legal advice for the Citizen Information Project (CIP).[36] This explained that statutory powers could be used to achieve a compulsory data sharing objective for a "public administration" purpose and described a mechanism which would remain consistent within the requirements of the Human Rights and Data Protection Acts. It was then realised that if data sharing could be based on the use of statutory powers without the need for consent, then you might as well integrate the CIP into an ID Card scheme which, after all, was a system based on compulsion and statutory powers with respect to its law enforcement and security function. One suspects this change in policy towards compulsion also underpins the Government's "Vision Statement"[37] on general data sharing and the debate as to whether patients can opt-out of the Summary Care Record.[38]

It is important to note that there are philosophical differences when a public authority is in control and when an individual is in control. For example, where a public authority is in control, it is likely to ask "who am I dealing with? I don't need permission to find out or to disclose personal details".[39] By contrast, when an individual is in control, the issue could be "I have chosen to reveal my identity to you because I want a service from you, but I don't want you to share my new address" or "I don't want your service so I am not going to tell you who I am".

[33] A sample of these are referenced in the text in the Appendix.

[34] From Mr David Blunkett to Mr Charles Clarke.

[35] Privacy and data-sharing. the way forward for public services (PIU report April 2002), paragraphs 10.24–10.33.

[36] The legal advice is contained in Annex 8 of the CIP final report (on http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp).

[37] Information Sharing Vision Statement (on http://www.dca.gov.uk/foi/sharing/information-sharing.pdf) is to justify data sharing in terms of "in the public interest". This is a likely reference to the phrase "necessary in the public interest" which is defined in S.42 of the ID Card Act 2006 which links to the "efficient and effective delivery of public services".

[38] See the web-site for "TheBigOptOut.org". It can be argued that the trust argument condenses to the issue of who is in control of medical records. Most patients think the GP is in control—that is until they become aware of Section 251 of the NHS Act 2006 which puts the Secretary of State in control of patient information. The question then is whether trust is maintained when the Secretary of State exercises that control without patient consent or GP involvement.

[39] The notion of seeking consent is nonsensical for most law enforcement, terrorist incidents, life threatening emergencies etc.

The position with respect to consent also differs. Where public bodies are in control of the data sharing, the notion of consent is in largely irrelevant because consent is absent, or because there are special circumstances where it is known that consent cannot be obtained.[40] If, however, individuals consent or have an easy objection to data sharing, implicit in that relationship is the fact that individuals can trust the sharing process, for if that trust is absent, then the sharing does not occur (or is stopped). Finally, it is worth point out that a lack of trust will arise when public authorities do things which the individual thinks should be under his or her own control.

April 2007

Annex

Timeline of the Decision to Use the NIR as a Population Register

Trust and surveillance

In this Annex, I show when decisions were taken to use the National Identity Register (NIR) of the ID Card as a population register. Since a population register is a form of surveillance, consideration of the issues surrounding a population register illuminates the issues of "trust" and "consent" which are central to the debate about a surveillance state.

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)[41] and which is intended to extend to private sector information (eg opening a bank account, hire of a car).

The decision to widen the use of the NIR to include a population register fundamentally changes surveillance role. 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.

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 30 issues of this nature.[42]

The basis of this analysis in this Annex has been published in *Data Protection and Privacy Practice(July 2006)*, but it has been updated and fully cross referenced for the Committee. That updating has unearthed further information which has not been published.

2002 and 2004—The public consultations deny wide use of ID Card database

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".[43]

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

[40] Criminals do not consent to data about them being exchanged between law enforcement agencies; neither do individuals whose medical details need to be shared because they are unconscious.

[41] 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.

[42] 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

[43] *Entitlement Cards and Identity Fraud*, Cm 5557, paragraph 2.40.

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).

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".

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.[44] In relation to a population register, a further public consultation was promised "to explore the issues around public acceptability of the proposal".[45]

April 2003—Legal advice and the CIP

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").[46] 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.

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".

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.

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

Clause 1 of the draft ID Card Bill[47] 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.

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.

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.

[44] 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".

[45] Paragraph 3.20 of CM 6178 ("Legislation on Identity Cards").

[46] Annex 8 is on http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp

[47] Published in April 2004 in CM 6178.

March–June 2004—CIP is separate from NIR

There is further evidence which suggests the two schemes were originally seen as separate. For example, the CIP Project Definition[48] prepared for CIP meetings in Spring 2004 identified around thirty 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.[49]

Other evidence also supports the view that the CIP and NIR were seen as separate:

- **29 March 2004**[50] 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:**[51] 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:**[52] 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)

Using the NIR as a population register was always a possibility—March 2004

A document made available to CIP personnel in March 2004[53] 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".

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

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[54] 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[55] 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)".

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".

---

[48] 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

[49] CIPP(04)12—"Towards a Legal Strategy" on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp

[50] Answer to PQ 163155, 29 March 2004.

[51] From http://www.gro.gov.uk/cip/Definition/ProjectBoardMinutes/index.asp

[52] From http://www.gro.gov.uk/cip/Definition/ProjectBoardMinutes/index.asp (Minutes confusingly posted under the date of 21 July).

[53] CIPP(04)12—"Towards a Legal Strategy" on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp

[54] Citizen Information Project: CIP progress report—10 September 2004 on http://www.gro.gov.uk/cip/Definition/ProjectBoardPapers/index.asp

[55] David Blunkett MP was Home Secretary till mid-December 2004, then from that date, Charles Clarke MP.

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". 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

A preliminary Privacy Impact Assessment (PIA) for the CIP was finalised in September 2004 (published in "Final Report, Annex 8: Legal issues")[56] 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.

Given the 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[57] as expressing interest in the PIA for the CIP's population register.

End of September 2004—a status summary

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.[58]
- 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 replied to the Home Affairs Committee ID Card Report

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".[59] As the NIR is *not* an *existing* register, this statement cannot refer the NIR which had not yet been created.

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

[56] Annex 8 is on http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp
[57] The minutes of 25 November 2005.
[58] see CIPPB(04)12—reference 53.
[59] Paragraph 44 of CM 6359.

the 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".

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.

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)

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.

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

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"[60] 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).

Similarly, paragraph 26 of the RIA (dealing with longer term benefits) did not mention the 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: as this function was specifically outlined as part of the CIP in the legal advice of April 2003, it is difficult to imagine that some cost estimates did not exist).

March—April 2005 CIP benefits form fifth of ID Card business case

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".

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.

[60] Paragraphs 64–72 of the Assessment.

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.

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

After the General Election, on May 25, 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 (Tony McNulty MP) signed an "updated version" of the Bill's Regulatory Impact Assessment (RIA) to inform subsequent Parliamentary debate on the Bill.

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

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 up-loaded 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".

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"(page 17). The CIP final 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).

These opportunities were:

- "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".

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.

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

A draft list of recommendations were prepared by civil servants for the CIP Project Board ("Submission to Ministers—draft")[61] to consider to send to ministers; the list showed that CIP officials were very aware of the privacy and constitutional issues.

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

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).

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.

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.

19 July 2005—ID Card Bill Committee stage (Commons)

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",[62]

20 Jul 2005—Response to written question, column 1783W

The following written question illuminates what was to be the "denial line" adopted by Government with respect to the use of the NIR for public administration purposes (until 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)

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,[63] 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

[61] CIPPB(05)45 dated 21 June 2005.

[62] 19 July, ninth sitting morning, Column 363 (Standing Committee *Hansard*).

[63] *Hansard*, 5 October 2005, Column 2845W.

Reading debate on the Bill, on 18 October, the Home Secretary[64] (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".

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—Joint Committee on Human Rights

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.[65] 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".

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

The House of Lords Delegated Powers and Regulatory Reform Committee, in its Fifth Report[66] 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,[67] 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".

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 Jan 2006—Lords Committee Stage: no explanation of CIP functionality

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).

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)

[64] *Hansard, October 2005 (Column 799).*
[65] Joint Committee On Human Rights (First Report), section 4, session 2005–06.
[66] Session 2005–06, 10 November.
[67] Appendix 1 of the above report.

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.

March 2006—a game of Parliamentary ping-pong

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.

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".[68]

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

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[69] 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"

In an open letter, Tony Blair promoted the widespread public administration use of the NIR database. He told Home Secretary John Reid[70] "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.

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

The term "national identity management" is being used by Government to represent 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). Page 7&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"

[68] *Hansard*, 29 Mar 2006: Column 1000.
[69] *Hansard*, 53WS, 18 April 2006.
[70] http://www.pm.gov.uk/output/Page9461.asp

This 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**[71] The opportunities of wider use of the NIR for CIP purposes are 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

According to Home Office Ministers,[72] 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".

It is interesting to note that one of the original Government consultations[73] 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.

APPENDIX 4

Memorandum submitted by R A Collinge

SUMMARY

The submission argues:

For the protection of individual liberty the powers of the state to gather information on its citizens need to be restricted, controlled and if possible rolled back. Assumptions are made that vast data gathering schemes will be more effective than more conventional approaches which may be both more efficient and cheaper means of addressing undoubted problems.

There is a fundamental difference between private information gathering which the citizen can, with adequate information, choose to join or not and the data gathered compulsorily by the state.

Particular care also needs to given to the control of CCTV and other data collected by various bodies without the individual having the ability to object.

1. One starts from an assumption that the executive of government has, in this country and elsewhere, understandably sought to increase its power in order to achieve its objectives. Reaction to this inevitable pressure has resulted in documents such as the Magna Carta and much more recently the Human Rights Act. Politicians will always argue that their proposals are fair and reasonable and that they would in no way misuse them. Unfortunately history does not bear this out.

2. The gathering of information is seen as one of the main ways in which power can be increased. It will in all cases be for "good reason" but the development of the national identity data base, amongst others, will fundamentally change the relationship between the individual and the state. The state will become the master of its citizens rather than their servant undertaking solely tasks than can be better done at that state level.

It should not be necessary to argue any further for restrictions on the capacity of the state to intrude on the privacy of its citizens but given that the Identity Card Act has been made law by a Parliament apparently oblivious of its historical responsibilities to control the executive it is necessary to respond further to this form of surveillance and others.

3. There is a fundamental difference between private data bases and the state sponsored ones. The state will require compulsory ID cards and the consequent entries in the National Database whilst private ones are voluntary. We can all choose to opt out of private schemes by avoiding credit, loyalty and store cards etc.

---

[71] See 24 June 2005 timeline entry "Final meeting of the CIP project".
[72] Answer to Mr Hoban's PQ 127212, 13 March 20.
[73] "Legislation on Identity Cards: A consultation", paragraph 3.20 (CM 6178).

4. *Private Databases*

The key guideline here is that the individual is given the maximum information as to how his or her data are to be used: that he or she can restrict the use of these data and that the system is satisfactorily regulated. Warnings should be given that the data are at risk from criminals and others who will inevitably find ways to steal data. The more data there are in any one place the more the incentive to find ways of stealing them.

There should be an absolute ban on any privately held data being available to any government department or agency.

5. *Government databases*

The Human Rights Act allows "interferences" with the general right to privacy if that "interference":

— is "in accordance with the law"

— has "legitimate objectives" such as national security, public safety, economic wellbeing, the prevention of crime , the protection of health or morals or the protections of rights or freedoms of others; and

— is "necessary in a Democratic Society".

Clearly these wordings are open to very wide interpretations and will need very close scrutiny. For example one mans "morals" may well be another's anathema. George Orwell warned against "Thought police".

Thus there need to be very tight restrictions on the gathering and use of information which the state will be gathering compulsorily. Access to law to determine whether the Act has been complied with will be essential, but appears at risk because of the restrictions currently being placed on legal aid. If real access is available then such things as the sharing of data between government departments and agencies may be controllable. Government data should never be available to private bodies.

The relevant Registrar may need enhanced powers to police these records.

Particular areas for concern include the gathering of information on children, the retention of DNA records by police even though an individual may not even have been charged , the practical difficulty of having a record corrected, the fact that no system of "profiling" has yet been able to cope with the infinitely variable nature of human beings, the certainty that the records will be criminally misused and the likelihood—from the evidence of history—that the costs of collecting data will far exceed all estimates. Has proper thought been given to the possibility that many of the claimed advantages of the sorts of record keeping and surveillance being promulgated could be better achieved by more conventional means such as more police or even a new body of border police? For example one Home Secretary accepted that identity cards would not have prevented the London bombers.

6. *Other surveillance*

CCTV is more used in this country than anywhere else. Tighter controls need to be in place to regulate the circumstances in which it can be used. Criteria need to be developed to decide how and when both public and private surveillance of this nature is essential and has real value. In practice is it avoided by criminals who are aware of it? How long can or should tapes of such surveillance be retained and by whom? What controls are there on the use of such records by persons other than those making the record?

7. *Road pricing*

It has been suggested that national road pricing be introduced under a scheme which will require all vehicles to be monitored at all times. It is impossible to overstate the concern that this brings in giving a myriad of officials the power to find out where any vehicle was at any time. Such a level of surveillance would have been welcomed by the Stasi amongst others.

The costs of such a scheme would be enormous. Why apparently is so little attention paid to the wide range of actions which could be undertaken at relatively little cost instead? Perhaps it is because it is easier and more rewarding to put forward one big idea whatever its cost in every sense rather than address such minutiae. These actions could include:

— free school buses—an enormous potential reduction in congestion;

— extension of the Manchester Metro which has been talked about for many years but nothing is done;

— slip roads at all possible junctions to allow traffic to filter to the left; and

— Crossrail.

And many many others all over the country which would reduce congestion relatively easily and without the enormous risks to "our way of life".

8. *Summary*

This country has been "sleep walking "into a surveillance society for a number of years. Real efforts now need to be made to ensure that the very nature of "our way of life" which the Prime Minister seeks to protect is not subverted from within.

April 2007

APPENDIX 5

Memorandum submitted by the British Medical Association

The British Medical Association (BMA) welcomes the opportunity to submit evidence to the Home Affairs Committee inquiry into "A Surveillance Society?".

The enclosed response focuses on the situation in England and includes input from the BMA's Working Party on NHS IT, the Patients Liaison Group (PLG), the Medical Ethics Committee (MEC), the Joint GP IT Committee of the General Practitioners Committee (GPC) and the Royal College of General Practitioners (RCGP), the Central Consultants and Specialists Committee (CCSC), the Junior Doctors Committee (JDC), the Medical Students Committee (MSC), the Staff and Associate Specialist Committee (SASC), the Forensic Medicine Committee (FMC) and the Medical Academics and Specialists Committee (MASC).

1. The British Medical Association (BMA) is an independent trade union and voluntary professional association which represents doctors from all branches of medicine all over the UK. It has a total membership of over 138,000.

2. The area of this inquiry on which the BMA would like to comment is that of the Department of Health's planned NHS Care Record Service which will give access to the medical and care records of patients across different NHS organisations. The already available information includes demographic details and is also due to include medications, prescriptions, social information and details of all medical interventions. The BMA supports the greater sharing of healthcare information between healthcare professionals to support patient care. We have concerns, however, over the implications of patient databases being used in the fight against crime or being abused by criminal access.

Access by Public Agencies to Private Databases

3. Since 1996 the police have had access to the Prescription Pricing Authority database. Although access to medical records by the police is currently possible in certain circumstances, in practice, it is a complex procedure to view a patient record and there is no direct police access to a database. Currently, access to a patient record requires knowledge of who the patient's GP is and then a Police and Criminal Evidence (PACE) production order from a judge if it can be proved that the material may be relevant evidence. This is still no guarantee that information will be available as treatment may have taken place in a variety of settings.

4. Due to the existence of the Personal Demographics Service (PDS), patient demographics are available already through one point of contact. After the implementation of the NHS Care Records Service, this data will be hugely supplemented. This must not alter existing policy and guidance on disclosure of information to the police.[74] NHS Connecting for Health has frequently publicly stated that police and other agencies will not have direct access to NHS data or to the new NHS database. There is much public mistrust and the BMA would strongly resist moves to allow direct access.

5. The BMA welcomes the decision to exclude NHS patient records from the Serious Crime Bill.

Data-sharing Between Government Departments and Agencies

6. The primary function of the NHS Care Records Service is to provide care for patients and the BMA would strongly oppose any plans to allow other government agencies access to the NHS Care Records Service, for example, the Home Office. There are other more appropriate routes for information sharing, when necessary, with these agencies. Allowing other agencies access would undermine trust in the system and the doctor/patient relationship. If patients are fearful that their healthcare information will be accessed by other agencies, they may withhold information, which could jeopardise their care and which could also have far greater public health implications. A further public health implication (besides patients withholding information that may put others at risk) is that if trust is lost in the system and information withheld, then incomplete or inaccurate data may be recorded that not only threatens individual patient care, but also the use of aggregated data for health services planning and epidemiological research.

[74] Both the BMA and the GMC have produced guidance on allowing third party access to health records.

7. The BMA has expressed concerns about healthcare information being included on identity cards to the Home Office. The BMA believes there should be no health information on identity cards for reasons of confidentiality and accuracy of the information.

Existing Safeguards for Data Use and Whether they are Strong Enough

8. No system is ever one hundred per cent secure and a potential threat remains from hackers. The BMA believes that the technical security arrangements for the NHS Care Record Service provide a sound basis requiring only modest changes to provide the technical support required to meet confidentiality standards. Following testing, any system must be carefully piloted in order to evaluate whether safeguards are strong enough.

9. With all databases it is important that the general public are properly informed about how their data will be held so that, if they have concerns, they can make alternative arrangements for their data, where appropriate.

Monitoring of Abuses

10. There is a real difficulty in detecting inappropriate access to confidential medical records. The traditional audit trail requires IT experts to examine an individual record and then attempt to discover whether access was necessary. Without involving professionals in confidentiality and audit, we do not see this as a realistic check.

11. Alerts will be an important confidentiality control providing some reassurance to patients that inappropriate access to summary and detailed records will be identified and addressed. They will also provide an important deterrence to staff from accessing confidential information where the circumstances do not justify it. Alerts will only be effective if action is taken when appropriate. We note that a commitment that all alerts are reviewed is included in the Care Record Guarantee (Commitments 11 & 12).[75] The BMA consider that this review process will be very important to protect confidentiality and promote public confidence in the NHS CRS.

12. The BMA has already raised concerns with NHS Connecting for Health over the funding and resourcing of Caldicott Guardians and privacy officers. The BMA welcomes the establishment of the Caldicott Guardian Council, and the recent publication *The Caldicott Guardian Manual 2006*. We have not yet seen any plans put in place to make any realistic estimates of the numbers involved, or to consider the resources that will be necessary to service them, and budget for additional resources if necessary. Without such an exercise, the BMA is concerned that local NHS organisations, and in particular their Caldicott Guardian functions, will be inundated and forced to ignore many alerts and therefore undermine a key confidentiality control. We understand that NHS Connecting for Health is currently undertaking a review of how the Caldicott Guardian roles will operate in consultation with Trust's and PCT's. This needs to be clarified if there is to be public and clinical confidence in the system.

Potential Abuse of Private Databases by Criminals

13. Criminals will have ways of attempting to access the system which may include bribing NHS staff or telephoning staff and pretending to be a patient or healthcare professional to access the record. Our concerns are that this will become easier as the numbers who can access a record are increased with a staff member being able to access any NHS patient's record, including address, health and social details and other sensitive information. Strict protocols must be in place to identify any telephone callers eg asking what organisation they belong to, the reason for requesting information and their organisation's telephone number for the NHS staff member to ring back.

14. There must be strict penalties for anyone who attempts to inappropriately access the NHS Care Records Service both from within the NHS and from hackers. We would recommend that staff found to have deliberately breached the confidentiality code should face strong disciplinary action.

April 2007

---

[75] http://www.connectingforhealth.nhs.uk/crdb/docs/crs—guarantee

APPENDIX 6

Memorandum submitted by the Audit Commission

The Audit Commission is an independent body responsible for ensuring that public money is spent economically, efficiently and effectively, to achieve high-quality local services for the public. Our remit covers around 11,000 bodies in England, which between them spend more than £180 billion of public money each year. Our work covers local government, health, housing, community safety and fire and rescue services.

As an independent watchdog, we provide important information on the quality of public services. As a driving force for improvement in those services, we provide practical recommendations and spread best practice. As an independent auditor, we ensure that public services are good value for money and that public money is properly spent.

Executive Summary

1. The Audit Commission welcomes the Home Affairs Committee's focus on data sharing and is pleased to submit evidence to its inquiry on "A Surveillance Society?"

2. This submission contains information about the scope of the Commission's National Fraud Initiative (NFI) as it currently stands and an indication of how it could be extended by the Serious Crime Bill currently before Parliament. After a brief introduction and a section about the development of the NFI, the submission is structured around four of the headings set out in the Committee's announcement of the inquiry: access by public agencies to private databases; data sharing between government departments and agencies; safeguards for data use; and profiling.

3. The Commission's NFI is a data matching exercise carried out every two years as part of the statutory audit of local authorities and NHS bodies. The NFI matches datasets including the audited body's payroll, student awards and loans, housing benefits, housing rents, the blue badge parking scheme for the disabled and single person council tax discounts to identify possible anomalies that could indicate fraud or erroneous overpayment.

Introduction

4. The UK economy faces an increasing challenge from fraudsters. Recent estimates in a report commissioned by the Association of Chief Police Officers, *The Nature, Extent and Economic Impact of Fraud in the UK*, place annual losses from fraud at £13.9 billion. These losses range from low value claimant fraud to high value, orchestrated and sometimes international fraud on all sectors of the economy.

5. The volume of cases and the scale of the more complex frauds require the use of technical solutions, and data sharing and matching are at the forefront of these.

6. The Commission's NFI is a data matching exercise carried out every two years as part of the statutory audit of local authorities and NHS bodies. The NFI has resulted in the detection of more than £300 million of fraud and overpayments since it began in 1998, and this figure is likely to exceed £500 million by the close of the current 2006–07 NFI exercise in May 2008. The Commission is a world leader in the use of data matching techniques, and we believe that such methods are invaluable in protecting the public purse.

7. The success of the NFI can be measured in part by the range of risk areas now being reported to the Commission for inclusion in the NFI. These range from abuse of occupational pension schemes and state benefits to procurement fraud. Where any of these areas emerge successfully from pilot exercises, they may be included in the NFI portfolio.

Detailed Response

Development of the NFI

8. The NFI is currently conducted as an audit exercise under the Audit Commission Act 1998 ("the Act"). Auditors must, among other tasks, satisfy themselves that bodies subject to audit, such as local government and NHS trusts, have put in place arrangements to secure the economic, efficient and effective use of their resources. In addition, auditors must comply with the *Code of Audit Practice* approved by Parliament under section 4 of the Act (http://www.audit-commission.gov.uk/reports/NATIONALREPORT.asp?CategoryID=&ProdID=CD9EFFCE-FD24-43fc-B54E-4C6E1BCC2ED4). Auditors' duties include identifying illegal items of account; identifying risks relating to the use of resources by audited bodies; and providing reasonable assurance that financial statements are free from material mis-statement, whether caused by fraud or other irregularities. Data-matching assists in identifying where such anomalies may have arisen, for further investigation by both the auditor and the audited body.

9. Auditors have powers under section 6 of the Act to obtain information that relates to a body subject to audit, where this is necessary for the purposes of undertaking the audit. This is the mechanism by which the auditor is able to obtain the data sets that are used in the NFI.

10. At the outset of the NFI in 1998, the data shared and processed by the Commission came almost exclusively from the audited bodies themselves, and the results from the data matches were returned to those participants. We used datasets including the audited body's payroll, student awards and loans, housing benefits and housing rents, and matched them to identify possible anomalies that could indicate fraud or erroneous overpayment. This included, for example, council tenants who had more than one council property and benefit claimants who had failed to declare their income from other sources.

11. Since 2000, we have added new datasets to address a number of emerging risks faced by audited bodies, such as abuse of the blue badge parking scheme for the disabled and single person council tax discount fraud. We have also introduced data from the Home Office and the Foreign and Commonwealth Office that detects employees of audited bodies who are not entitled to work in the UK and benefit claimants who are not entitled to claim public funds. These matches help local authorities to detect housing and council tax benefit fraud and to identify employees who have no right to live or work in the UK.

12. The Serious Crime Bill (currently at Report stage in the House of Lords) contains provisions that could place the NFI on a broader statutory footing, so that it will no longer be conducted simply as an audit exercise. Rather, the Commission itself will have powers to undertake data matching for the purposes of preventing and detecting fraud, so that both public and private sector bodies can participate in the benefits of this exercise more generally. The Commission will decide which data sets should be matched on the basis of its knowledge and experience of where fraud is likely to be either serious or prevalent, informed by pilot exercises where appropriate.

Access by Public Agencies to Private Databases

13. Under the Act as it currently stands, the NFI is restricted to collecting and matching data that "elates to bodies subject to audit". This therefore excludes a large amount of data that is held by both public and private sector bodies.

14. However, Clause 65 Schedule 6 of the Serious Crime Bill provides a statutory gateway that will allow both private and public sector[76] bodies to contribute data voluntarily to the Commission for the purposes of data matching. Such data can only be provided if the Commission believes it to be appropriate for the purposes of preventing and detecting fraud, and bodies will not be able to share patient data voluntarily under this provision. All data matching must comply with the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. This power will be enabling; private and public sector bodies will be under no obligation to provide this information to the Commission.

Data Sharing Between Government Departments and Agencies

15. The Serious Crime Bill provisions for the NFI would enable government departments and agencies to use the NFI as a conduit for data sharing to address local and national fraud risks in a controlled, secure and well regulated environment. Clause 65 Schedule 6 of the Bill provides that bodies subject to the Commission's audit and inspection regime must provide their data to the Commission for data-matching. Other public bodies can do so on a voluntary basis (as outlined above).

Safeguards for Data Use

16. The Commission has adopted a range of methods to ensure that the data matching process is managed at all times in a way that is proportionate and secure, and that data subjects are advised of the use of their data. The principal methods include:

- distributing a *Code of Data Matching Practice* governing all aspects of NFI data matching to all participating bodies and making it available on the Commission's website at http://www.audit-commission.gov.uk/nfi/codeofdmp. This Code reflects the core underlying principle that personal data will only be obtained and processed in accordance with the Data Protection Act 1998. Clause 65 Schedule 6 of the Serious Crime Bill could place a statutory duty on the Commission to produce a *Code of Data Matching Practice*, and for all those who are participating in data matching exercises to have regard to the Code. The Commission could be required to consult with all its audited and inspected bodies and any other body it considers appropriate; this would always include the Information Commissioner, who has written the foreword to the current Code;
- extracting from each dataset only the minimum fields required for effective fraud detection. Handbooks with data specifications can be found at http://www.audit-commission.gov.uk/nfi/handbooks.asp;
- requiring participating bodies to notify data subjects about the inclusion of their data in NFI;

[76] Excluding those bodies that are within the Commission's audit and inspection regime; with the exception of registered social landlords, these bodies will be under a mandatory duty to participate in NFI.

— making no assumptions as to whether or not an individual has been involved in fraudulent activities. Instead, anomalies that are detected as a result of data-matching are referred back to the relevant participating body for further investigation, and clear guidance is given to the relevant bodies and their auditors that they should treat all matches as anomalies to be checked, rather than being proof that fraud has occurred;

— holding data under strict security and destroying and rendering it irrecoverable at the end of each exercise;

— releasing data matches through a secure website, access to which is carefully monitored;

— ensuring that each participating body can only access its own matches and that investigators have their access restricted to those match types for which they are responsible;

— piloting new datasets and risk areas prior to their inclusion in NFI, and only including them if warranted by the value or number of frauds they detect;

— monitoring the results of investigations to ensure that any data no longer considered essential to fraud detection is left out of future data submissions; and

— keeping site security at our data centre permanently under review.

17. It is the Commission's intention that these principles will continue to apply to the new provisions under the Serious Crime Bill if they come into effect. We believe that they provide an appropriate balance between restricting intrusion into the privacy of citizens and protecting the public purse against fraud. There will also be additional protections under the new provisions. These include tight restrictions on the circumstances in which data can be disclosed, and tough criminal sanctions for disclosure in breach of these requirements.

18. There will also be specific restrictions on the use of patient data within NFI, which will be limited to uncovering fraud within the NHS only, and it will not be permissible to disclose any further than necessary for that purpose. In fact, clinical patient data is not used within the NFI because it is not relevant to fraud.

Profiling

19. While the NFI concentrates primarily on data matching to detect fraud, there are instances where data mining (a search across multiple datasets for patterns that might suggest organised fraud) is also effective, particularly where patterns of abuse may emerge over a large number of participating bodies. However, this technique is employed exclusively to detect existing, rather than predict future, fraud. The Commission does not intend to profile individuals according to their behaviour and characteristics in order to predict their future likelihood or propensity to commit offences. The use of mining techniques to profile fraudsters and thereby predict future fraudulent behaviour is controversial, unproven and not considered appropriate to the NFI.

April 2007

APPENDIX 7

Memorandum submitted by The Institution of Engineering and Technology

The Institution of Engineering and Technology (IET) is pleased to respond to the Home Affairs Committee consultation on "A Surveillance Society".

The IET was formed in March 2006 through a merger of the Institution of Electrical Engineers (IEE) and the Institution of Incorporated Engineers (IIE). The IET has in excess of 150,000 members worldwide drawn from a broad range of science and engineering disciplines. The membership represents a wide range of expertise, from technical experts to business leaders, encompassing a wealth of professional experience and knowledge, independent of commercial interests.

Introduction

1. The best advice the IET can give the Committee is to consult the excellent report published in March 2007 by the Royal Academy of Engineering, entitled *Dilemmas of Privacy and Security*. Several of the Working Group members who produced this report are Fellows of the IET and we endorse their report as a comprehensive and thoughtful study.

2. Arriving at an acceptable balance between security and privacy requires dialogue and understanding between policy makers, technologists and the public. As members of the Committee are in a prime position to influence this dialogue, we give our views below on where the responsibilities should lie.

Technology Considerations

3. The fundamental principles of security are already well documented and understood. Every database is vulnerable to data corruption and data theft. These risks become very significant if the database is widely accessible, particularly if it is connected to the Internet. In these circumstances, if the database contains personal data about many people, or vulnerable people, the database access software should be developed to very high standards of security engineering. The necessary standards far exceed normal commercial software quality.

Responsibilities of Policy Makers and Officials

4. It is important to remember that databases are an implementation technology, not an end in themselves. In each instance, it is vital to analyse and define the desired outcomes and the business changes that are needed to achieve these outcomes, before deciding whether a new database is a suitable solution and moving on to define its scope. Any such project should be managed as a business change project enabled by technology, not as a technology development project.

Role of Parliament

5. MPs need to be very clear about what they are aiming to achieve and what the specific outcomes of legislation will be, including the level of security/risk. It should be the role of MPs to ensure that all legislative changes are checked in detail for security/risk, and to understand the implications of this, before they are approved.

6. The IET is well placed to advise on the critical technical aspects of legislative changes.

Conclusion

7. The report *Dilemmas of Privacy and Surveillance*, published last month by the Royal Academy of Engineering, aims to ensure that policy makers, government and other organisations are aware of the potential problems so that they can be prepared to confront them. It also offers suggestions for technological and regulatory solutions to privacy issues which are intended to stimulate debate and research into protecting and designing for privacy.

8. The IET commends this report to the Committee.[77]

April 2007

APPENDIX 8

Memorandum submitted by the London School of Economics and Political Science Identity Project

Executive Summary

1. This submission presents an assessment by the LSE Identity Project team on the way that the Identity Cards Scheme, as currently envisaged by the Home Office, is furthering the creation of a surveillance society. The team has identified three main aspects of the Scheme that it believes are directly contributing to a surveillance society, as defined by the recent report commissioned by the Information Commissioner's Office.[78] These are: the design decisions underlying the Scheme; the biographical footprint checking associated with enrolment into the Scheme and the apparent lack of security underlying the implementation of the Scheme.

2. That is, the Scheme is explicitly designed to maximize the surveillance capabilities of identity cards in ways that other countries find unacceptable; the process of enrolment into the Scheme involves bringing together data from a dispersed set of existing databases and once this information has been collected, the Home Office seems unprepared to ensure that it is accessed securely, in accordance with existing best practice guidelines and the legal requirements of the Data Protection Act. Thus, our analysis suggests that there isn't just a tendency to govern but a tendency for surveillance, even at the expense of good governance.

---

[77] *Dilemmas of Privacy and Security—Challenges of Technological Change.* Royal Academy of Engineering, March 2007. http://www.raeng.org.uk/policy/reports/default/htm

[78] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf September 2006. A similar point on privacy by design is made in the Royal Academy of Engineering report on the Dilemmas of Privacy and Surveillance: Challenges of technological change. http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf March 2007.

About the LSE Identity Project

3. The LSE Identity Project[79] provides ongoing research and analysis into the UK Government's proposals to introduce national biometric identity cards. The *main* Identity Project report[80] 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, ongoing national and international media coverage, and was frequently cited during debates in both Houses of Parliament.

4. Since the publication of the *main* Report in June 2005, the 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 about the ongoing costs of the Scheme as the government prepares for procurement. They have also analyzed the Strategic Action Plan released in December 2006 when the government presented a near-complete rethink of its implementation plans for the identity cards scheme, explicitly citing the criticisms presented by the Identity Project that the scheme was "high risk and too expensive".

5. 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 analysing the policy landscape for identity policy in Canada.

6. Members of the LSE Identity Project have published 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. These are available on the project website.

Surveillance by Design

7. Although George Orwell's "Big Brother" is the most common representation of the surveillance state, Neil Postman[81] argues that it is Aldous Huxley's image of the Brave New World that is more sinister: "In the Huxleyan prophecy, Big Brother does not watch us, by his choice. We watch him, by ours. There is no need for wardens or gates or Ministries of Truth".[82] That is, the risk is that we explicitly design and build the surveillance state ourselves.

8. There are a number of aspects of the Identity Cards Scheme that deliberately include *surveillance by design*. These can be easily identified by comparing the UK Scheme with similar proposals for identity cards in other countries. Many of these design features are a direct consequence of the Scheme being designed and implemented by the Home Office with its policy agendas encompassing crime prevention, passports and identity fraud. In other countries identity cards are generally designed to ease the administrative processes for both the individual and the state, rather than being a form of surveillance.

9. For operational reasons, the Home Office has decided to link enrolment into the National Identity Register with the issuing / renewal of passports. One claimed benefit of this process is that it is intended that the Identity Card will be usable as a travel document, at least within Europe.[83]

---

[79] http://identityproject.lse.ac.uk

[80] http://identityproject.lse.ac.uk/mainreport.pdf

[81] Postman Neil (1992) Technopoly: *The surrender of culture to technology*. Vintage Books, New York. (ISBN 0-679-74540-8); Postman Neil (1985) *Amusing ourselves to death: Public discourse in the age of showbusiness*. Methuen, London. (ISBN 0-413-40440-4).

[82] Postman (1985) Pages 160–161.

[83] Eg Baroness Scotland, *Hansard* 12 December 2005 Column 974 "The identity card will be available for those who wish to travel in Europe. One will not need a passport to travel to any EU country but you will need a passport for other international travel—to America, New Zealand, Australia or anywhere outside the EU. The identity card will be very convenient. Noble Lords will know that many mainland European nationals use their identity cards to travel within the EU area. Our system of identity card will have the same facility. The noble Lord will remember that it is proposed that the identity card should cost about £30, which is a great deal cheaper than a passport. For those who tend not to travel outside the EU, that may be a considerable advantage".

[84] Eg"There are additional EU requirements specifying that by 2009 ePassports should include fingerprint data which will require personal attendance for fingerprint enrolment. 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* so that it can participate in the development of the EU regulations and maintain the security of the British passport on a par with other major EU nations" NAO Report on the introduction of ePassports, HC 152 Session 2006–2007, section 1.7 Emphasis added, see also http://ec.europa.eu/idabc/en/document/6806/194 "Two fingerprints or 10?".

10. Although there is currently *no legal obligation* on the UK to include iris or fingerprint biometrics in travel documents,[84] the Identity Card Scheme has used the likely future international obligations requiring the inclusion *images* of fingerprints on travel documents as a basis for collecting and storing the fingerprints of all UK residents and comparing *templates* of these fingerprints against all those previously registered with the Scheme.

11. It is claimed that this will help ensure that no individual can register with the Scheme more than once (although this goal is likely to be more easily achieved by the use of (comparatively more expensive and less well understood) iris scanning technologies). Yet no other country is implementing a similar scheme. No other country is implementing iris scans for their identity cards or passports, and to our knowledge no other country is taking all ten fingerprints from their citizens for this purpose.

12. In such circumstances, the insistence on collecting fingerprints is unclear. Perhaps the most honest justification for this was provided in an email from the Prime Minister, to those who had signed a petition against the introduction of identity cards: "The National Identity Register will help police bring those guilty of serious crimes to justice. They will be able, for example, to compare the fingerprints found at the scene of some 900,000 unsolved crimes against the information held on the register."[85] This is an instance of the government designing for surveillance rather than for easing public administrative burdens for both the citizen and the state.

13. The future international obligations on travel documents will apply to other countries. Many, however, have made very different design decisions about the collection and use of this personal data.

14. The French, for example, have a long history of identity documents, numbers, and markings. In 1987 the French introduced a new identity card, made of plastic and designated as "secure". This is the form of the current national ID card. It is not mandatory and, while a fingerprint is taken, it is not digitized and does not appear on the card. It is stored securely, and only on paper. While it can be accessed by a judge, in a specific case where the police already have identified a suspect, the conditions for access to the fingerprint are tightly regulated. A central database has been introduced, but it is limited only to the delivery of the card system.[86]

15. Germany provides one of the most interesting examples of identity cards. Most Germans readily carry around their identity cards but, because of past abuses, are also quite wary of the collection of personal information by the Government. Under Federal Data Protection Law, the Federal Government is forbidden from creating a back–end database of biometrics for the identity card. That is, German privacy law prevents the creation of the kind of central database envisaged for the UK. Instead, any information that is collected for the ID card system is stored locally at the registration offices. A private contractor, Bundesdruckerei GmbH, uses this information to issue the card, but as soon as the document is completed, all personal data is deleted and destroyed.[87]

16. France explicitly does not use a single identifier to link government records across departments and countries do not maintain a detailed audit trail of every time the identity of the card holder is formally verified. Indeed, documents released by the Department for Work and Pensions under Freedom of Information legislation[88] suggests that early versions of the design for the Scheme allowed for local ("offline") verification of PINs and biometrics (ie not against the National Identity Register and hence not appearing on the central audit trail of verifications). This design choice appears to have been overturned in the current version.

Centralised Collection of Biographical Data and Government "Registration Centres"

17. In order to ensure that the National Identity Register does not contain duplicate records for any individual, the Home Office has decided to combine checking the biometrics of individuals registering with the Scheme against all the biometrics currently stored in the database, with detailed "biographical footprint checks".[89]

---

[84] Eg"There are additional EU requirements specifying that by 2009 ePassports should include fingerprint data which will require personal attendance for fingerprint enrolment. 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* so that it can participate in the development of the EU regulations and maintain the security of the British passport on a par with other major EU nations" NAO Report on the introduction of ePassports, HC 152 Session 2006–2007**,** section 1.7 Emphasis added, see also http://ec.europa.eu/idabc/en/document/6806/194 "Two fingerprints or 10?".

[85] Tony Blair, PM's response to ID cards petition, 2007 Archived at http://www.pm.gov.uk/output/Page10987.asp

[86] LSE Identity Project Main Report Pages 66–70.

[87] LSE Identity Project Main Report Pages 70–72.

[88] http://www.dwp.gov.uk/pub—scheme/2007/apr/.

[89] With the decision not to include iris scanning as part of the biometric verification process, the role of the biographical footprint verification becomes more important as Katherine Courtney told the Science and Technology Select Committee: "You cannot record someone's fingerprints if they do not have any fingers. That is a known limitation and one of the reasons behind our intention to use multiple biometrics to try to overcome that limitation" Answer to Q302.

18. Biographical footprint checks involve face–to–face interviews with registrants of 10–20 minutes duration. "At the interview, customers will be asked basic information about themselves—not deeply private information, but information that can be checked to confirm that they are who they say they are".[90]

19. These interviews will initially be targeted a first time applicants for passports, taking place at the 69 new interview centre locations.[91] This is based on UKIPS assumptions of 600,000 first time passport applicants per year.[92] In comparison, they are expecting 4,220,000 new and renewed passports in 2010–11, all of which will need to be subject to authentication by interview before they can be issued with Identity Cards. News reports suggest that the questions will be drawn from a list of 200 possible questions.[93]

20. This news report continues: "Applicants will be asked to confirm facts about themselves which someone attempting to steal their identity may not know but to which the interviewers already know the answer. Mr Herdan (executive director of the Identity and Passport Service) said there would be no pass or fail mark but officials would make a judgment on the basis of the whole interview whether an applicant was telling the truth".[94] The process will involve "third party authentication of biographical information".[95]

21. This again illustrates the Home Office's tendency for surveillance by design: For the Home Office questions to be meaningful, it would need to collect the data from these databases before putting the questions about the data to the individual.

22. This means, at the very least, that the interviewers will have access to vast amounts of personal information about each individual enrolling in the scheme. The practical implementation of this process would involve collating this information at the interview location, before the interview begins. There appears to be no formal guarantee that this collated information will be destroyed after use and that it will not be misused.

Security of the National Identity Register

23. The LSE Identity Project *main* Report warned[96] of the security risks of storing all the data associated with the National Identity Register in a single, centralized database. Senior representatives from industry have offered similar assessments.

24. The Strategic Action Plan issued in December 2006 indicates that the data will now be held in three distinct databases, relating to the three main elements of the data being held:[97] biometric information, biographical information and technical information. Each set of data is to be stored, at least temporarily, in an existing database. It is unclear as to whether these existing databases have previously been designed to be as secure as is likely to be required for the Identity Cards Scheme.

25. A recent Cabinet Office report,[98] on Identity Risk Management for e–government services suggests a series of different levels of security required for different kinds of identity management risks for e–government services. It provides guidance about how to address the risks associated with each level.

26. The risk assessment process is given in Supplement E, where scores are allocated for different kinds of threat factors. Even the most generous account of the likely risks to be faced by Identity Cards Scheme, would give the Scheme a risk level three: "the highest potential impact in cases of possibly falsified or mistaken identity for online services. The likely impacts here include damage to property, severe embarrassment to an individual, significant financial harm to an organisation (including the service provider) and possibly physical harm to individuals" . . . "Level Three represents the most sensitive kinds of service which should be brought online given the inherent nature of the Internet and its users. Where the risk exceeds the ceiling for this group, then the viability of the service as an online offering should be reviewed. For Level Three services there is always a requirement for string initial proof of identity and strong authentication in service delivery".[99]

---

[90] http://www.passport.gov.uk/downloads/Introduction—of—Passport—Application—Interviews.pdf Page 3.

[91] Aberdeen, Aberystwyth, Andover, Armagh, Barnstaple, Belfast, Berwick-upon-Tweed, Birmingham, Blackburn, Boston, Bournemouth, Bristol, Bury St. Edmunds, Camborne, Carlisle, Chelmsford, Cheltenham, Coleraine, Crawley, Derby, Dover, Dumfries, Dundee, Edinburgh, Exeter, Galashiels, Glasgow, Hastings, Hull, Inverness, Ipswich, Kendal, Kilmarnock, Kings Lynn, Leeds, Leicester, Lincoln, Liverpool, London, Luton, Maidstone, Manchester, Middlesbrough, Newcastle, Newport, Newport (Isle of Wight), Northallerton, Northampton, Norwich, Oban, Omagh, Oxford, Peterborough, Plymouth, Portsmouth, Reading, Scarborough, Shrewsbury, Sheffield, St Austell, Stirling, Stoke-on-Trent, Swansea, Swindon, Warwick, Wick, Wrexham, Yeovil and York.

[92] Page 10.

[93] http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/03/21/npass21.xml

[94] *Ibid.* Emphasis added.

[95] This term is used in the UKIPS Business Plan 2007–2017 page 10. It is not clear to us whether this term is meant to include existing government databases as well as those provided by commercial organisations such as Equifax. According to a recent written answer, the Personal Identity Process (PIP) currently checks an individuals records against: Electoral roll; BT records; Credit records; County court judgments (1999); HALO deaths—a database compiled from Governmental and funeral directors' records; ONS deaths (England and Wales 1983–2003) [122006].

[96] Chapter 14.

[97] http://www.identitycards.gov.uk/downloads/Strategic—Action—Plan.pdf Para 15.

[98] Identity Risk Management for e-Government Services, http://www.cabinetoffice.gov.uk/csia/documents/risk—mgt/id—risk—mgt061127.pdf

[99] Page 8.

27. Although it is arguable that the risks associated with the NIR are higher than is covered in this guidance document (ie because any security breaches could have an impact on many people, not just isolated individuals which appears to be the main focus of Level Three), the advice about Level Three authentication (ie someone who is in the system confirming their identity) is instructive:

> "Clients will authenticate themselves to the system by the presentation of a digital certificate. This will be held in an access token, which would ideally be a smart card, token or mobile device. Clients will demonstrate their right to that credential through the use of a private key, and a password or biometric. The system will authenticate users based on the validity of public key/private key pairs, and on the validity of the credential. Username/password combinations are not acceptable for Level 3 authentication".[100]

28. Compare this guidance with recent (2007) Home Office descriptions about how users will access the Scheme:

> "There will be a number of different methods of verifying identity under the National Identity Scheme ranging from a visual check of the card, which will not require a card reader, to card authentication, PIN verification and up to biometric verification where a high level of identity assurance is required".[101]

> "Design work with potential users of the identity verification service remains ongoing. As such, it is not possible to state which services and information will be available online to ID card holders through the use of a personal identification number at this time".[102]

29. Thus, the Home Office continues to be determined to build a system that is inherently insecure. Moreover, important questions of legal liability that arise from the potential misuse of the Scheme[103] have not yet been addressed, and even UKIPS appears to be repositioning itself as "the preferred supplier of identity services"[104] compared to earlier claims to provide the "gold standard of identity".[105]

April 2007

APPENDIX 9

Memorandum submitted by the Joint Council for the Welfare of Immigrants

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 has 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 assure 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 public services. 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

[100] Page 18, emphasis added.
[101] Joan Ryan, Written answer to question by Mr Hoban 120387.
[102] John Reid, Written answer to Mr Clegg 119612.
[103] http://www.computerweekly.com/Articles/2006/12/19/220759/who-will-foot-the-bill-for-id-card-fraud.htm
[104] UKIPS business plan 2007–17 page 5.
[105] Eg Baroness Scotland, *Hansard* 16 January 2006 Column 484; Lord Bassam of Brighton, *Hansard* 12 December 2005 Column 1098.

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 is discriminatory and will conflict with the UK's obligations under national treaties and conventions.

The Joint Committee on Human Rights 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."

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).

Legal opinion sought by JCWI concurs with that of the JCHR. In addition counsel 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 UCRC. 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 operations 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 biometric documentation and information and deny 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
— conflict with implementation of progressive equality cultures by public sector and the third sector.

April 2007

APPENDIX 10

Memorandum submitted by CIFAS the UK's Fraud Prevention Service

SUMMARY

1. CIFAS—The UK's Fraud Prevention Service welcomes the opportunity to submit evidence to the Home Affairs Committee's inquiry entitled "A Surveillance Society?". CIFAS is an independent not-for-profit membership association, set up as a company limited by guarantee, that allows the exchange of information on applications, accounts and insurance claims that have either been made fraudulently or are being used fraudulently.

2. This evidence explores the current benefits and safeguards involved in data sharing within the private sector, as undertaken by those organisations who are already Members of CIFAS, and also proposals for data sharing with the public sector. It also sets out our suggestions for criteria that will be key to the effective sharing of data between the public and private sectors.

SHARING OF DATA

3. Fraud knows no boundaries. Professional criminals do not care from whom they take money—they attack wherever and whenever an opportunity arises. Fraud losses suffered by the private sector can mean that prices increase and tax revenues fall. Equally, losses suffered by the public sector can reduce the ability to provide public services. Sharing data about fraud is a very good way—and often the only practical way—to prevent such losses and help identify those responsible—namely criminals who will continue to use the same false identities and illegal methods as long as they are effective. Sharing details about these will reduce the opportunity for criminals to profit.

4. Pilot data matching exercises between the public and private sectors undertaken by CIFAS have proved that many of those who commit fraud against the private sector also commit fraud against the public sector.[106] Sharing data on fraudsters will lead to earlier detection and prevention of fraudulent activity.

5. The types of fraud that can be prevented through data sharing within both the public and private sectors are not limited to identity theft, the focus of much of the current media coverage on fraud. Also covered are application frauds and insurance claim frauds, which involve a real person who misrepresents his or her entitlement or status, and which can have as large an overall cost to the UK economy as frauds involving identity.

6. Across the private sector, the sharing of data is a long-established and effective method of preventing and detecting fraud proactively. The 260 CIFAS Member organisations share data on identified frauds in the fight to prevent further fraud and, by doing so, avoided losses during 2006 totalling £790 million. This figure represents an increase year on year of 16%.

7. CIFAS welcomed the overall conclusions of the Government's Fraud Review, and would support the establishment of a National Fraud Reporting Centre.

STANDARDS AND EVIDENCE

8. Since the inception of CIFAS in 1988, Members have always followed strict rules regarding the sharing of data. The CIFAS operating model has been developed in consultation with the Information Commissioner.

9. CIFAS recognises that there must be clear standards relating to the nature of the information that is shared. There must be a defined burden of proof for determining fraud and a high level of accuracy must be upheld. There must also be strong safeguards to maintain the security and proportionality of data that is shared. Such measures will be key to ensuring the consent and support of both the general public and the

[106] Home Office, *New Powers Against Organised and Financial Crime* (Cm 6875–July 2006), Chapter 1.

Information Commissioner's Office. However, it is important that the detail of these measures should not be put into the public domain, as to do so could give criminals the knowledge required to circumvent the processes.

10. All data shared through CIFAS has to be backed by sufficient evidence to support a formal report to the police or other relevant law enforcement agency, although sharing data through CIFAS is not a replacement for a report to the police. Before sharing details of a fraud or attempted fraud, the CIFAS Member will have identified a criminal offence, having either suffered, or potentially suffered, a loss and will have sufficient grounds to press criminal charges.

11. The information that is shared through CIFAS is limited to that which will be of relevance to the prevention and detection of further frauds. Only factually correct and accurate information may be shared and will not include any expressions of opinions by the CIFAS Member. Details of racial or ethnic origin are not shared, and neither are details of political or religious beliefs.

Transparency

12. It is important that individuals are clearly made aware of the uses to which their data could be put. In order to comply with the fair processing principle of the Data Protection Act 1998, current CIFAS Members include a "fair processing notice" in all customer contracts. This clearly defines the nature and purpose of the information sharing that occurs between CIFAS Members. Similar notification would be essential for any future public-private data sharing, regardless of the mechanism used.

13. Similarly, individuals must be told how to access, and if necessary correct, any information held about them. As the extent of data sharing grows, this becomes increasingly important. The use of inaccurate data is self-defeating, risks the loss of public confidence and would breach data protection law. Published complaints procedures and clear methods for individuals to access any data held about them are key to this.

14. CIFAS Members successfully resolve the majority of complaints they receive about the use of CIFAS data directly with the individual concerned. Only in a handful of cases has CIFAS found that the Member did not act according to the rules.

15. CIFAS is run on not-for-profit principles and any financial surplus is always ploughed back into the services delivered to Member organisations. The current CIFAS Members are banks and building societies and other suppliers of secured/unsecured credit to consumers and businesses, along with share dealing, leasing and hire, communications and insurance companies. Membership is *not* open to intermediaries, such as brokers, independent financial advisers, loss adjusters, or to debt collection agencies, tracing agents and private investigators. Public authorities and utilities are able to join, subject to having appropriate legal powers to share data for the purposes of fraud prevention and detection.

Use of Data

16. The prevention and detection of fraud needs to be proactive to be most effective. Limiting the sharing of data to cases where a suspicion of fraud already exists would curtail potential benefits. That is not to say that a "blacklist" of people involved in fraud should be created; rather that it should be normal procedure for any request or application for a public sector benefit/service to be checked against those who have committed fraud previously. This is what has been happening in the private sector for many years to great positive effect.

17. Every two years the Audit Commission runs the National Fraud Initiative (NFI), a data matching exercise that detects frauds and overpayments. Using data from a number of different public bodies, the 2004/05 exercise detected £111 million worth of fraud and overpayments—but only after the event, when the money had been lost. The proactive sharing of data, as opposed to the retrospective matching of data, would enable such frauds against the public sector to be prevented before money is lost.

18. A proactive method of fraud prevention provided by CIFAS is the Protective Registration Service. This service, frequently recommended by the police, allows those who are at risk from identity fraud to put a protective warning against their address. The risk could arise from the theft of personal identification documents (eg during a burglary) or following a breach of security (eg the loss of a computer containing payroll data). The protective warning alerts CIFAS Members to take extra care when receiving new applications from that address, which could involve requesting further proof of identity.

19. CIFAS information is processed by a number of participating fraud prevention agencies that also provide CIFAS Members with fraud prevention services. When a Member identifies a fraud, a warning is placed against the addresses linked to the application/proposal/claim or account/policy/service. The warning shows the name used on the application/proposal/claim or account/policy/service but this does not necessarily mean that the person named is involved in the fraud, as fraudsters tend to use a variety of names, some false and some genuine.

20. The CIFAS warning will appear on the fraud prevention agency record of any person who has a link with the address, and any CIFAS Member subsequently checking that address will see the warning. Matching data for fraud prevention purposes using just the address, rather than a name at an address, is a proportionate response to the threat posed by fraud, particularly fraud involving identity. The added value of this matching has been proven consistently.

21. The process that results from sharing information about a previously identified fraud must be fair and consistent, yet also robust enough to ensure its effectiveness. Any CIFAS Member that sees a CIFAS warning is required to take extra precautions to ensure that the application or account that prompted the search is genuine. No CIFAS Member organisation that receives a CIFAS warning from the system when checking an application or account is allowed *automatically* to refuse to supply the facility, product or service because of the warning—an appropriately trained member of staff must make the decision after due consideration.

22. The value of the shared information is related to its age. Although historical information can have value, the sharing of current data will be of much greater benefit and will be more compliant with the fifth Data Protection Act 1998 principle.

Onward Transmission of Data

23. Data that has been shared by a CIFAS Member is only shared with other CIFAS Members—it is not passed on to anyone else. Organisations who are not Members but also use a participating fraud prevention agency would not see any CIFAS warnings. This concept of reciprocity is essential to the long term success of any data sharing system.

24. The police and other law enforcement officers are able to request data from CIFAS but only on a case-by-case basis. Section 29 of the Data Protection Act 1998 permits disclosure of data for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders.

25. The Social Security Fraud Act 2001 gave the power for authorised Department for Work and Pensions officers and for authorised local authority officers to obtain information from certain types of organisations, including CIFAS. Authorised officers can obtain any information relevant to the prevention and detection of benefit fraud in tightly defined circumstances as set out in a Code of Practice.

26. Whilst there have been large scale data matching exercises successfully undertaken using CIFAS data,[107] no personal data was disclosed as part of those pilots. Any profiles of fraudsters based upon the data shared between CIFAS Member organisations have not been shared with law enforcement agencies.

27. Any proposed data sharing through CIFAS between the public and private sectors would still occur under the existing practices and procedures outlined previously. Neither the source, destination or nature of the information shared would materially alter the standards or safeguards applied.

Misuse of Data

28. Information on those identified as being involved in fraud is also valuable to the criminal community, as it could be used to circumvent measures put in place to prevent fraud. The misuse of data can arise from both internal and external threats.

29. Although many external threats can be managed through the use of appropriate hardware, software and physical security tools, internal threats (ie employee fraud) are more complex to deal with. Best practice among CIFAS Members for vetting prospective employees includes references for—and the full verification of—employment history, the verification of any qualifications, and verification of identity to the same standard as for anti-money laundering checks. CIFAS has recently launched a staff fraud database for Members and, in conjunction with the Chartered Institute of Personnel and Development, has also provided Members with a guide to tackling staff fraud and dishonesty.

30. The wrongful disclosure of data is an offence under Section 55 of the Data Protection Act 1998 and other legislation. CIFAS welcomes the proposed increases in the penalties for this offence recently announced by the Department for Constitutional Affairs.

Data Sharing and Surveillance

31. As used in the CIFAS operating model, the sharing of data cannot be considered surveillance as the sharing only occurs after a fraud (whether attempted or successful) has been identified. It is important, however, to strike the right balance between the operational need for confidentiality and the public need to be open about how fraud is prevented. To maximise the likelihood of the successful apprehension and prosecution of offenders, customers are not advised when a CIFAS warning is placed in the majority of cases. Data protection legislation has still been observed as customers will have already been notified by a "fair processing notice" that details of any identified frauds may be passed to fraud prevention agencies.

[107] *ibid.*

Conclusions

32. CIFAS suggests that the following criteria are key to the effective sharing of data between the public and private sectors:

- The sharing of data needs to be proactive, but only information relevant to the prevention of fraud should be shared.
- There needs to be a defined burden of proof which is satisfied before sharing takes place.
- Individuals must be made aware of the possible uses of their data.
- Automatic refusals should not be made purely on the basis of data that has been shared.

33. Sharing data for the purposes of preventing and detecting fraud offers the potential for great benefits to UK citizens, the private sector and public authorities. The full potential can only be realised with the minimum of impact on individual liberty, however, where there are clear standards and safeguards in place to govern this sharing.

April 2007

APPENDIX 11

Memorandum submitted by Mr Charles Farrier

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 rise in technology combined with a mass media-fuelled climate of fear threatens our way of life. Citizens of the UK are asked to sacrifice privacy for measures that it is not possible to prove the success of. The sudden increase in surveillance technology threatens the citizen's right to privacy and their very way of life. The use of surveillance on law abiding citizens going about their daily business or exercising their democratic right to protest calls into question the health of our democracy. The forthcoming National Identity Register and the government's data sharing agenda will remove existing privacy firewalls. The use of such data for profiling is the stuff of despotism. If surveillance is allowed to increase unchecked then it could have effects on the behaviour of individuals who are anxious not to stand out in the crowd or appear in a bad light in the eyes of the authorities. Stronger safeguards must be put in place, bills before parliament should be subject to privacy impact assessments and our constitution needs to be strengthened to protect the citizen.

Introduction

2. We live in dangerous times, as the rise in technology combined with a mass media-fuelled climate of fear threaten our way of life. The world of performance targets, blame and litigiousness forces officials and decision-makers to "do something", to err on the side of perceived safety. The fear of "not acting" is made to weigh heavy on minds but at what cost?

3. As Zbigniew Brzezinski, former National Security Advisor to Jimmy Carter recently put it: "Fear obscures reason, intensifies emotions and makes it easier for demagogic politicians to mobilize the public on behalf of the policies they want to pursue."[108]

4. A recently published policy review document released by the government states: "Citizens are asked to accept the gathering of greater levels of information and intelligence in the knowledge that this will facilitate improvements in public safety and law enforcement."[109] Why should citizens accept further intrusion into their private lives when research calls into question the effectiveness of current measures? It is interesting to note that the huge proliferation of CCTV cameras led to just a 5% reduction in crime whilst street lighting led to a 20% reduction.[110]

5. Chief amongst the current armoury of so-called safety measures is the use of surveillance technology. A way of intruding into people's lives in the interest of "protecting" them. After all, the axiom "nothing to hide nothing to fear" rules supreme, doesn't it? I will argue that there is very much to fear, particularly if you have nothing to hide.

[108] Zbigniew Brzezinski—"Terrorized by 'War on Terror'—How a Three-Word Mantra Has Undermined America", *Washington Post* Sunday, March 25, 2007; Page B01 (http://www.washingtonpost.com/wp-dyn/content/article/2007/03/23/AR2007032301613.html)

[109] "Building on progress: Security, crime and justice", HM Government Policy Review, March 2007.

[110] "To CCTV or not to CCTV?", NACRO, June 2002 (http://www.nacro.org.uk/data/resources/nacro-2004120299.pdf)

Privacy

6. Privacy is a difficult concept to define and something that many people seem to take for granted. In the UK privacy is embodied by the system of common law—in which you are free to do anything as long as it is not specifically legislated against. Privacy goes hand in hand with anonymity. Buying a newspaper is not an unlawful act and may be done under anonymity by making a cash transaction in a small newsagent. But consider this simple act in the modern world. The journey to the newsagent filmed on CCTV, the purchase filmed within the shop and the transaction recorded if the purchase is made with a credit or debit card. Why should this be watched and recorded? Now imagine a future world in which this information is added to a central register and the choice of newspaper contributes to a profiling score. Such a vision is not far off with the UK National Identity Register waiting in the wings.[111] What have we become that we feel the need to pry into the lives of law abiding citizens in such a way?

Technology

7. The start of the 21st century has ushered in a wave of "modernisation" often for the sake of it. Those that do not embrace "modernity" are branded Luddites. Yet many of the changes in surveillance technology are so far reaching that they threaten what it is to be human. For instance, advances in CCTV cameras mean that we will progress from simple stop motion black and white images to high resolution, colour digital images with facial recognition and perhaps soon expressions recognition.[112] Technologies such as expression recognition will intrude into behaviour identity and lead to a robot-like neutral public persona. Technology should be a tool to assist humanity not a weapon with which to enslave it. Advances in technology are big business and there is a whole industry keen to make whatever case necessary to increase sales—governments should be acting on behalf of their citizens not the commercial designs of the high tech industry.

8. For an insight into surveillance technology trends and their impact in modern society I draw the committee's attention to the Institute for Prospective Technologies (IPTS) report *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*.[113].

Surveilling Dissent

9. One of the most worrying trends in recent years has been the photographing and filming of protesters.[114] Our society is supposedly a democracy in which the right to protest is respected. Yet law abiding citizens who choose to go on a demonstration are routinely filmed. The eerie sight of police with handheld equipment recording the presence of protesters embodies a threatening and disapproving state. This is unacceptable in a democracy. What laws allowed this to become routine? What has our society become that the expression of a democratic right is met with such muscle-flexing of the state? What happens when the advances in technology allow the previously shot footage to be matched against the National Identity Register using facial recognition? Will this data be used for profiling? Protesters should be heard but not individually monitored and any existing footage should be destroyed.

Identity Management

10. Identity management is a cornerstone in the surveillance state. Through the introduction of a centralised database of all citizens, each allocated a unique identifier (National Identity Register Number, NIRN), the full power of total surveillance is unleashed.

11. In the past identifying information such as fingerprints and mugshots has only been stored for convicted criminals but the UK's identity scheme seeks to store such personal and private information on all members of society. The unique identifier will allow information from disparate databases to be combined.

Databases and Data Sharing

12. The indexing of data by the NIRN when combined with the government's forthcoming data sharing agenda[115] will destroy existing privacy firewalls. For instance, assurances that medical data will not be stored on the National Identity Register are meaningless if medical records contain a reference to a citizen's unique identifier. Effectively the National Identity Register will be joined to the NHS spine via the NIRN.

[111] Whilst such proposals are not on the face of the Identity Cards Act, it could be possible through the linking of databases (upon the customer's unique identifier) to data mine in this way.

[112] See "Urban Surveillance and Panopticism: will we recognize the facial recognition society?" by Mitchell Gray http://www.surveillance-and-society.org/articles1(3)/facial.pdf

[113] *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, A Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS July 2003 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf)

[114] See *Casualty of War—eight weeks of counter-terrorism in rural England*, Liberty, July 2003 (http://www.liberty-human-rights.org.uk/publications/pdfs/casualty-of-war-final.pdf)

[115] See *Information sharing vision statement*, HM Government, September 2006 (http://www.dca.gov.uk/foi/sharing/information-sharing.pdf)

13. The government promised a consultation on data sharing and a data sharing bill in the Spring of 2004. Why did they not fulfil this promise? Surely if they have nothing to hide they would have done—surely they have nothing to fear from explaining to UK citizens the full implications of data sharing. Why are they introducing such measures by stealth?

14. In addition, the audit trail enshrined in the Identity Card Act will facilitate the creation of dossiers on UK citizens. Each time a card is electronically read it will be possible to record the location in time of that event and so track individuals and their behaviour.

Profiling

15. The collection of information in databases is intrinsically linked with profiling. Roger Clarke of the Australian National University defines profiling as: "a data surveillance technique which is little-understood and ill-documented, but increasingly used. It is a means of generating suspects or prospects from within a large population, and involves inferring a set of characteristics of a particular class of person from past experience, then searching data-holdings for individuals with a close fit to that set of characteristics".[116]

16. Allowing computers to categorise citizens in this way is a frightening vision of a future in which every action could increase the likelihood of becoming a suspect. In addition, computers always make mistakes and it will only be a matter of time before such systems lead to wrongful arrests, detentions and imprisonments.

17. Profiling is the stuff of despotism. In Nazi Germany the forerunner to modern computers, the Hollerith punch card machine was used to categorise the German population in the census of 1939.[117] This allowed them to conduct the Holocaust in a controlled and systematic way.

18. The unwritten constitution of Britain is too weak to protect UK citizens. The power of parliament is supreme and armed with such technology it is not difficult to see a future "elective dictatorship" completing the erosion of civil liberties that has been accelerating so alarmingly in recent years.

19. Lord Scarman, the first chairman of the Law Commission warned: "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."[118]

The Electronic Panopticon and its Side Effects

20. The advances in surveillance technology will create an electronic Panopticon in which citizens feel that their every move is being recorded and analysed. The effect of this will be to create a society of behavioural uniformity. The law abiding citizen clearly stands to lose the most. As *New York Times* columnist William Safire put it: "To be watched at all times, especially when doing nothing seriously wrong, is to be afflicted with a creepy feeling. That is what is felt by a convict in an always-lighted cell. It is the pervasive, inescapable feeling of being unfree."[119]

Conclusions

21. The government should be protecting privacy not working to destroy it as it currently is. There should be legislation against excessive surveillance. Safeguards should be put in place and sunset clauses for all measures that reduce citizens' freedom. All bills before Parliament should be subject to a privacy impact assessment.

22. The constitution needs urgently to be reinforced to create clear limits on what the government can and cannot do. As Christian Parenti put it: "As a society, we want to say: Here you may not go. Here you may not trade and analyze information and build dossiers. There are risks in social anonymity, but the risks of omniscient and omnipotent state and corporate power are far worse."[120]

April 2007

---

[116] *Profiling: A Hidden Challenge to the Regulation of Data Surveillance* by Roger Clarke, Visiting Fellow, Department of Computer Science, Australian National University, 1995 (http://www.anu.edu.au/people/Roger.Clarke/DV/PaperProfiling.html)

[117] See *IBM and the Holocaust* by Edwin Black, 2002, Time Warner Paperbacks.

[118] Hamlyn Lectures, English Law—The New Dimension, 1974.

[119] *The Great Unwatched*, William Safire, *New York Times* 18 February 2002. 12 December 2002.

[120] *The Soft Cage—Surveillance in America* by Christian Parenti, 2003, Basic Books.

APPENDIX 12

Memorandum submitted by Ross Johnson

Executive Summary

- The shift in the authority of surveillance from public to private will continue. The most significant danger arises from private access to public data, and not the reverse. In return for the provision of such access, private bodies could agree to disclose data they hold to public agencies. Most people will encounter surveillance in larger part from private rather than public bodies. A major risk is that compliance with surveillance will bring its own rewards to the individual.
- The Government appears obsessed with data sharing. The amount of data and the number of persons and bodies to whom it is proposed access will be granted is on an entirely unprecedented scale. Ministers have a poor attitude towards rules designed to protect data from being shared too widely, and propose weak reasons for linking all departments in the transmission of personal information.
- Surveillance should become the subject of legislative regulation over and above current laws on data protection. Legislation should recognise the social and civil rights aspects of surveillance, and not merely the security of the data gathered by it. A new law should be introduced to provide for a "balancing" test in each case of surveillance. Reforms should also be made to current data protection law to provide for the better empowerment of the individual.
- Mass surveillance is becoming a pervasive problem, and needs to be checked. Aside from new regulation there should be a strongly-empowered regulator such as the Information Commissioner. Public understanding of the issue of surveillance and its importance to them needs to be improved.
- Increased data sharing and wider access to information will lead to more cases of criminal abuse, but the more important issue is what is happening legally.
- Privacy impact assessments should be introduced.
- Privacy-enhancing technologies are a good idea, but should not be relied upon.
- Profiling poses significant risks with potentially far-reaching, undesirable consequences.

Introduction

1. I submit this memorandum as written evidence to the Home Affairs Committee in its inquiry entitled "A Surveillance Society?" announced in its call for evidence on 27 March 2007.[121]

2. I am a member of the public who takes a particular interest in the subject matter of this inquiry. I have followed the Parliamentary progress of legislation such as the Identity Cards Act 2006, and have read about the wider issues in the media and other sources.

3. The memorandum includes a section on each of the points set out in the inquiry's terms of reference, and begins with an executive summary.

Access by Public Agencies to Private Databases

4. The Government's proposed National Identity Register (NIR) provides wide scope for intrusions of the State into private life. A detailed audit trail of the use of a NIR entry may be built up,[122] necessarily resulting in information that would otherwise be stored only in private databases becoming available to public authorities.

5. Examples of public use of private data beyond its stated purpose include the disclosure of Oyster card logs[123] and London Congestion Charge[124] information to the Metropolitan Police.

6. As the ICO report[125] points out at paragraph 26.2, we should assume that "the shift of power from public to private" will continue. I suggest to the Committee that the immediate danger is not greater use by public agencies of private data, but use by private bodies of public data. I agree with the report that private sector "governance", in particular commercial organisations and employers, will become increasingly

[121] HAC press notice no 18.
[122] Identity Card Act 2006 (c 15), Sch 1, para 9.
[123] *Oyster data is "new police tool"*, BBC News, 13 March 2006; http://news.bbc.co.uk/1/hi/england/london/4800490.stm
[124] *London charge zone is security cordon too, says mayor*, The Register, 17 February 2003; http://www.theregister.co.uk/2003/02/17/london—charge—zone—is—security/
[125] A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network, September 2006.
[126] *Ibid*, at para 3.9.

powerful.[126] One's day to day encounters with "authority" are with these bodies rather than the State, and the Government may sell or otherwise make available information to such bodies too freely; "44 000 user organisations" are expected to apply for access to the NIR.[127]

7. A very clear risk is that, in exchange for public data, the private sector could agree to make data it controls available to public bodies, so creating and perpetuating a dangerous cycle. Business and employers would together provide a great deal of detailed personal information.

8. I was most surprised when a colleague informed me that the supermarket chain Tesco charges its customers up to £70 for overstaying a limit of three hours in their car parks,[128] and uses ANPR[129] and the DVLA database to enforce it. This appears to be a flagrant abuse of personal data held for entirely unconnected purposes, yet it is legal[130] and a fee may be imposed for access.[131]

9. The danger posed by increasingly detailed and shared private databases is very well described in the ICO report, which speaks of "compliance bringing rewards".[132] We face devastatingly bad consequences if its predictions on personal RFID "chipping" are borne out. Becoming implanted to obtain "rewards" and discounts, and as a "status symbol,"[133] perfectly sums up the Information Commissioner's own description of "sleepwalking into a surveillance society".[134]

Data Sharing

10. The Government proposes a vast increase in data sharing powers beyond anything we have seen before. For example, the Digital Switchover (Disclosure of Information) Bill would authorise provision to the BBC and others of information about individuals such as dates of birth and National Insurance numbers in order to assist in upgrading their television sets.[135]

11. It is becoming increasingly popular to include data sharing powers in legislation, such as in the Serious Crime Bill,[136] the Statistics and Registration Service Bill[137] and the UK Borders Bill.[138] Sections 17 to 21 of the Identity Cards Act provide extensive powers for the unprecedented disclosure and duplication of information between a large number of public authorities.

12. The NIR itself is now to be constructed through data sharing,[139] as a cost-saving measure, despite its being originally heralded as a single, new, clean database.[140]

13. The Government have further announced the creation of a "single database" for the interface of the citizen with the State,[141] essentially total data sharing using the NIR as a basis. This is very widely opposed by the Opposition parties and the media; *The Sun* called it "an open invitation to fraud and corruption".

14. Consolidating all of our personal information into a single network and allowing access to it by an increasingly large number of operatives puts us at greater, not lesser, risk of identity theft and over-intrusive levels of surveillance. Data would be more vulnerable due to more frequent duplication and disclosure, and any benefit would be outweighed.

15. The Government points out that the NIR cannot contain certain types of data, such as DNA, but there is nothing to prevent the NIR Number being used to link from other databases such as the National DNA Database and the road pricing ANPR log of every car journey. There is also a desire to improve the quality of CCTV images in order that they can be linked to the NIR via the facial biometric.[142] Proposed fingerprint "fishing expeditions"[143] have serious implications for the burden of proof and our traditional liberties. The NIR audit log will gather a very detailed collection of evidence on innocent people, available for search at the State's convenience. The public interest does not justify such intrusion.

16. There is cause for concern when Ministers describe current data protection law restricting data sharing as "over zealous"[144] and, offensively, as a "barrier . . . to information sharing".[145]

---

[126] *Ibid*, at para 3.9.
[127] *Identity Card Technologies: Scientific Advice, Risk and Evidence*, House of Commons Select Committee on Science and Technology, 4 August 2006, HC (2005–06), at Appendix 15, para 7.
[128] HC Deb (2005–06), 14 December 2005, Vol 440, cols 451WH–458WH.
[129] "Automatic Number Plate Recognition", a CCTV system that recognises vehicle registration marks.
[130] Road Vehicles (Registration and Licensing) Regulations 2002, r 27(1)(e).
[131] Ibid, at r 27(2).
[132] At para 32.3.
[133] At footnote 232.
[134] *Watchdog's Big Brother UK warning*, BBC News, 16 August 2004; http://news.bbc.co.uk/1/hi/uk—politics/3568468.stm
[135] Explanatory Note, Bill 3 EN 06-07.
[136] HL Bill 27 2006–07, Schedule 6.
[137] Bill 8 2006–07, clause 38.
[138] Bill 53 2006–07, clauses 36–41.
[139] *Giant ID computer plan scrapped*, BBC News, 19 December 2006; http://news.bbc.co.uk/1/hi/uk—politics/6192419.stm
[140] Eg David Blunkett, HC Deb (2004–05), Vol 428, cols 377–387.
[141] *Whitehall plan for huge database*, BBC News, 14 January 2007; http://news.bbc.co.uk/1/hi/uk—politics/6260153.stm
[142] *"Better CCTV needed for ID" march*, BBC News, 11 May 2006; http://news.bbc.co.uk/1/hi/uk—politics/4761519.stm
[143] *Government response to petition "ID cards"*, 19 February 2007.
[144] *Ibid.*
[145] *Government spins data sharing*, The Register, 14 September 2006; http://www.theregister.co.uk/2006/09/14/dca—information—sharing/

17. In the provision of public services the Government appears very eager to collect, share and disclose information almost without limit, and the issue warrants very close attention.

Safeguards and Regulation

18. The Data Protection Act 1998 is often thought to offer more protection than it does. A particular example of note is the highly controversial issue of fingerprinting schoolchildren.[146] Nevertheless, the Act does provide us with a very good starting point in the protection of personal data.

19. I agree with the ICO report that the issue of "surveillance" is wider than that of mere "privacy", and propose that strong and robust new regulation should be introduced to guard against incursions on social principles such as human dignity and autonomy.

20. To create such a new regulatory regime a definition of surveillance will be required. I consider the comprehensive definition set out in the ICO report[147] to be a sound one.

21. I think the appropriate test to apply in regulation is one of "balance". An appropriate formulation may be that surveillance should only be permitted where it is a proportionate response to a given aim, in a similar vein to the qualified rights articles in the ECHR and, in one respect, the DPA.[148]

22. I think a word is due on one particular aspect of the DPA that I find unsatisfactory. Paragraph 1 of Schedule 2 provides a general "get out" where the data subject agrees to processing, which is used in some contracts of employment to provide for blanket agreement to data processing under the Act. Likewise agreement to data processing of any sort can be imposed as a condition for receiving goods or services, for example the provision of one's name and address. Such cases should be determined on the merits using paragraph 6(1), and the data controller should not be able to force agreement.

The Monitoring of Abuses

23. It is not hard to spot abuses. Barely a week seems to go by when Ceefax does not report some further extension proposed to the surveillance society; the latest is the idea of tagging dementia sufferers.[149] Such things together add up to the pervasive surveillance described in the ICO report.

24. We are seeing an increasingly large amount of data about innocent people being routinely, easily and cheaply logged.

25. We risk surveillance becoming normalised in the minds of future generations . As if we hadn't already seen enough de-sensitisation, there are now proposals to fingerprint for identification children aged 11 to 15,[150] a highly sinister move that the balance must clearly lie against.

26. Too often the purposes for which data is processed change after it has been collected, with those who defend the integrity of such data challenged to say why it should not, for example, be used in a police investigation.

27. There are anomalies in the balance. For example, whilst we have a proposed universal NIR, a DNA database containing details of millions of innocent people including children[151] and four million CCTV cameras, there is no requirement that CCTV systems themselves be registered.

28. "Mass surveillance" is becoming a pervasive problem.[152] with proposals now for CCTV systems that not only listen to what we say[153] but also tell us what to do.[154] That Hertfordshire's ANPR system runs every one of its scans through 40 different databases[155] is nothing short of frightening.

29. Yet the whole surveillance model does not eradicate social bads. Those who break the rules will continue to break the rules. It is the law-abiding who will provide the information to the authorities that can be used against them, as was seen recently with speeding.[156]

30. Public understanding of issues around privacy and surveillance needs to be improved. I found the point made in the ICO report about "slow social suicide"[157] very apt. An over-reliance on surveillance and requiring everyone to prove everything they claim leads to the rule of the computer and a downward spiral of impersonal dealings and mistrust. Yet there is a distinct lack of public concern.

---

[146] *Schools warned on fingerprinting*, BBC News, 7 February 2007.
[147] At paras 3.1–3.2.
[148] At Schedule 2, para. 6(1).
[149] *Tag dementia sufferers—minister*, BBC News, 19 April 2007; http://news.bbc.co.uk/1/hi/uk/6570511.stm
[150] *Child fingerprint plan considered*, BBC News, 4 March 2007; http://news.bbc.co.uk/1/hi/uk/6417565.stm
[151] *Under-18s DNA records to continue*, BBC News, 16 February 2006; http://news.bbc.co.uk/1/hi/uk—politics/4720328.stm
[152] *Mass surveillance—United Kingdom*, Wikipedia, the free encyclopedia; http://en.wikipedia.org/wiki/Mass—surveillance£United—Kingdom
[153] *Olympics audio surveillance row*, BBC News, 26 November 2006; http://news.bbc.co.uk/1/hi/uk—politics/6186348.stm
[154] *"Talking" CCTV scolds offenders*, BBC News, 4 April 2007; http://news.bbc.co.uk/1/hi/england/6524495.stm
[155] ICO report, para 10.4.5.
[156] *Camera-caught drivers not fined*, BBC News, 19 April 2007; http://news.bbc.co.uk/1/hi/uk/6568813.stm
[157] At para 2.8.2.

31. A particularly interesting case of public attitude arose this month at the Walkabout Inn in Cardiff,[158] where there were ID checks and data retention on all patrons of the pub for spurious reasons. In a rather chilling quote on the burden of proof, the deputy manager Kylie Scobie said,

> "There are two reasons people don't want to provide ID. Either they aren't old enough or they are planning to cause trouble".

32. The only proper way in which to address these problems is through the use of a strong statutory regulator, with the Information Commissioner being the obvious choice.

Potential Abuse of Private Databases by Criminals

33. I think the major issue that faces us is not fraudulent data use, but interference with our rights as citizens through entirely legal uses of surveillance by both public and private bodies.

34. Nevertheless, I have little doubt that the provision of access to an ever-increasing amount of data to an ever-increasing number of civil servants and others will only make for a higher risk of the theft and abuse of data. This would be a far cry from the stated intention of such reforms, which is ostensibly to somehow make us all safer.

Privacy Impact Assessments

35. I entirely approve of the concept of privacy impact assessments (PIAs), and support their introduction as a statutory requirement in cases involving surveillance. The ICO report definition I mentioned earlier would be the appropriate one to determine when the requirement is to apply.

36. Marx's questions, as set out in the Appendices to the ICO report, offer a comprehensive basis for conducting a PIA (or SIA). We must do what we can to ensure that a PIA/SIA is conducted rigorously and is effective in stopping or limiting excessive surveillance.

37. The concept is a very good one, though it should not replace the strong form of regulation that I have already proposed.

Privacy-Enhancing Technologies

38. Technologies used to protect and enhance privacy are a useful safeguard, which I support. We must not however consider them to be the end of the story, and they should not be used to justify things that would not have been acceptable without them.

Profiling

39. Before reading the ICO report I honestly had no idea of the extent to which both public and private bodies used profiling. Like the characters in the report's scenarios I was not aware of the amount of data that was held on me.

40. Profiling has the potential to make very significant impacts upon our lives. The image of estates separated by statistics is very easy to picture. The idea of "Personal Behaviour Schemes" set out in the ICO report[159] is I am afraid to say an entirely plausible one, the arguments for which I can imagine being made.

41. The potential of profiling for marketing is great, and may contribute to discrimination in the provision of goods and services.

42. Profiling gives a significant chunk of power to those in authority to question us on what we do and ask us to justify what they consider on their own criteria to be "unusual" behaviour. Whereas we ought only to be challenged if there is reasonable suspicion of an offence, this type of surveillance provides the means for essentially anything an operative chooses to form the basis of an investigation, and hence further surveillance, putting them in an increasingly powerful position. That is not the sort of society that I want to live in.

April 2007

---

[158] *Drinkers asked to have ID scanned*, icWales.co.uk, 16 April 2007; http://icwales.icnetwork.co.uk/southwalesecho/news/tm—headline=drinkers-asked-to-have-id-scanned&method=full&objectid=18912996&siteid=50082-name—page.html

[159] At para 32.2.

APPENDIX 13

Memorandum submitted by the Intelligent Transport Society for the United Kingdom

THE TRANSPORT PERSPECTIVE

Executive Summary

Transport comprises a major component of the public realm in the UK. The opportunities for surveillance in transport are therefore substantial. Furthermore, individuals tend to have no choice about exposing themselves to surveillance when using transport. Because of this, the transport environment constitutes a key focus for both policing and privacy issues.

Technology is affecting transport as much as any other sphere of UK life. As systems become more powerful, more mobile, and cheaper, these offer increased abilities for surveillance to be conducted, both legitimately and otherwise.

This note briefly reviews the nature of transport and the developing role of technology within it, before addressing the Committee's questions individually. As ITS (UK)—the respondent—is a systems-oriented trade body, our perspective will be technical rather than political.

1. *The transport context*

The transport context is large and multifaceted. Some of its key generic aspects are the following:

- Infrastructure: road and rail networks, waterways, stations, ports and airports. Technology is used to ensure that these are kept free-flowing, as far as possible, and any incident quickly identified and responded to.
- Public transport: services, and the operators that provide them. Technology is used to monitor their progress, and to advise travellers of changes (including disruptions).
- Freight and distribution: goods and materials are transported by private vehicles and fleets. Technology is used to track them, particularly where they are sensitive or hazardous.
- Private travel: individual vehicles, motorised and unmotorised, and individual travellers. Technology and services in this area are developing particularly rapidly, as economics make accessible what was previously available only to corporate users. It is currently used largely to access relevant travel information, but there are also a range of sensors and communications systems available.
- Regulation and enforcement: vehicle safety, vehicle/driver/passenger authorisation, and compliance with transport rules. Relevant use of technology includes reactive systems (for example, emissions testing at MoT) as well as active systems (for example, safety cameras).

2. *Technology in the transport context*

The use of technology in the transport context started early; ground to air voice communications and ("dumb") rail/traffic signals have been in existence for a long time. "Intelligent" controlled systems date from around the 1970s; sensor systems and the retention of historical data from around the late 1980s; and video from approximately the early 1990s. Surveillance technologies in transport are therefore a relatively recent development.

The pace of technology usage has not slackened. It is routine now for buses to be equipped with a number of CCTV cameras, and to record up to a month's worth of imagery on a local hard drive. The imagery might be from within the bus but might equally well be outward facing. The data provided by this is regularly exploited by the police and other security agencies. The same is true of static cameras at roadside or in stations, airports and filling station forecourts.

Non-imaging technology is also developing and being deployed rapidly. Smartcard ticketing (such as London's Oyster) enables identified individuals to be tracked through key points on the transport network and allows for the collected data to be stored, processed and shared. Vehicle identifiers do the same for cars; currently this is available through automatic number plate recognition (ANPR) systems that use cameras, but studies on more sophisticated electronic vehicle identification (EVI) systems have been underway within DfT and at DVLA for a number of years.

Perhaps the most dramatic change in transport relevant technology is the advent of powerful, personal systems: mobile phones. These can be used, unregulated, for capturing imagery throughout the transport system and, with a few excepted locations, to transmit such images immediately. They can also, as transmitting electronic devices, be used as trackable sensors, including covertly.

3. *Surveillance and the use of third party data*

The data collected through these means may provide useful information to those wishing to surveil, either with respect to specific target individuals/localities or with respect to general monitoring. This includes:

— Public agencies with a security remit;

— Private agencies with a security interest; and

— Agencies and individuals with no security remit.

In the first two cases, the legitimacy of access to data depends on the relevance of the data to the agency's operations, and also on the incidental residual risk of providing the data. In the third case, legitimacy may be referred to data protection ("I want to know what you have on me") or simply to freedom of information.

Data collection may "proactive" and open-ended, where security monitoring is the principal concern of an agency; or it may be "reactive", targeted and triggered by specific events, as where enforcement is the principal concern. It is much easier to put regulatory safeguards into the latter context, where the default is "no access".

4. *Access by public agencies to private databases*

"Private databases" come in a number of types.

— Data held by organisations as part of their own management. Scheduling data, engineering records, etc come into this category; so too do corporate security data, such as camera records.

— Data held by organisations as part of a public function. This includes data held by PFI management contractors: for instance, the National Traffic Control Centre, National Air Traffic Services, etc. It also includes data held by public bodies which has been provided by private sector organisations on a restricted use basis.

— Data held by individuals.

In the first case, access is normally available only as part of a warranted investigation, or where the data owner chooses to notify the public authorities. The lack of guidance in this area can may both processes cumbersome. A transport operator can suddenly find his information assets seized for investigation, and have little recourse to appeal; conversely, policing opportunities are likely to be lost because—say—a 'hot' vehicle is not identified by a private security system.

A partial exception to this lies in the British Transport Police operations on the rail network. The close day-to-day working between BTP and rail operators means that there is much greater clarity, by and large, over where database information may usefully be requested and provided. This function does not exist on the roads network.

In the second case, legitimate access by security agencies should be contractually assured, and any necessary limitation on access or procedural requirements applied at that time (with justification).

In the third case there is very little that can be done without an external reason.

In all three cases, the problem of constraining access to where it is legitimate is difficult (except where prearranged processes exist): once a decision has been taken to actively search a third party database, possibly without consent, the data is in principal fully available. Restriction at that point can only relate to the *subsequent use* of the data (eg how much can be revealed in court).

5. *Data sharing between government departments and agencies*

The UK is not good at sharing data between government departments and agencies.We believe that the public holds an expectation that, where *specific* information is available to government (in the widest sense), it should be used for all purposes which the public regards as legitimate. For instance, if a local authority street camera captures an image of a known criminal's vehicle, the police should be made aware of it. There are a number of ways of engineering this which stop short of allowing all government bodies full access to each others' databases.

There have been some positive steps towards information sharing between traffic managers and the police. However, outside London, this is still tentative; partly because systems are installed with transport funds for purely transport requirements, without taking security needs into account. More could be done to encourage joint projects at local level, for instance through good practice forums.

The problem of *generic* access to transport databases is more problematic. Intelligence and security agencies are, understandably, willing to ask transport departments to provide data only when they can be fairly specific and there is a clear operational urgency. There is potentially valuable information in operational databases that could be mined (eg for profiling). However this would require much freer access; it is not clear that this would have public support, but moreover it would impose a significant operational burden on both transport and intelligence functions which would need to be resourced.

6. *Existing safeguards for data use*

We do not see major problems with the safeguards currently in place; except to note that the need for caution might restrain legitimate usage.

We believe that the key driver to limit data sharing (apart from the need to address public concerns about privacy) derives not directly from its use in processing and analysis, but in the actions it might lead to. People are bothered by the fact that they might be "snooped on", but more bothered that they might suffer worse consequences as a result of misidentification. Identification based on smartcard ticketing or on vehicle number plates are both, of course, open to, and currently subject to, a number of caveats. Genuine mistakes, inertia by the user, or deliberate falsification, affect the accuracy of both.

Release of information to public media may need to be reviewed. In this respect, the Freedom of Information Act (and the surrounding policies) makes it distinctly harder to sustain data protection.

7. *Monitoring abuses*

Following on from the previous point, abuses (actual and potential) of available data are a significant reason that people are uncomfortable with data being shared. Data *abuse* therefore holds back legitimate data *use*.

A clever and determined person can subvert most operational practices, and it is not possible to prevent the possibility of (for example) a rogue policeman exploiting information available to him/her for personal ends.

This is partly a technical issue, but mostly one of management culture. Organisations need to be tougher on the misuse of data by their staff. There is an important lesson here: the current framework concentrates more on *institutional* rather than *individual* misuse.

8. *Potential abuse of private databases by criminals*

There are two ways in which criminals might abuse private databases:

— They might build their own private database (legitimately or otherwise), and use them for criminal purposes;

— They might exploit (openly or through hacking) or corrupt other peoples' databases.

There are many scenarios that might be envisaged; in most cases, system design has tried to reduce or mitigate the risk. For example, smartcard tickets on a bus or train could potentially be read by a criminal with a device in a briefcase, and personal data or money obtained; however, the use of encryption makes this problematic.

In some cases the risks are simply unclear. What could be achieved by a private number-plate camera, covertly positioned by a motorway? Or near a sensitive installation—say, a lab where animal testing happens? This requires an assessment of potential criminal opportunity.

9. *The case for introducing privacy impact assessments*

Privacy is a holistic concept; it is also (paradoxically) highly contextual to person, place, time, and nature of information.

It is not clear to us that there is a specific single way in which privacy impact assessment could be implemented to make it relevant to all circumstances. Therefore, it should be left up to individual scrutiny to determine whether and how to address privacy impacts.

10. *Profiling*

Profiling is an operational practice. We have little to say about this, other than to note that increasingly complex and sophisticated profiles will be possible as technology rolls out.

A related concept might be called "reverse profiling", and relates to differences in systems coverage or capability around the country. Some abuses might be more prevalent where detailed information is available to be exploited; others, where surveillance is less thorough. The traditional UK approach to this—create pilot sites and monitor them—seems to be a sensible approach to this.

11. *Conclusions*

The transport environment is only really beginning to adopt large systems that capture, store and use personal data. Until very recently travel was largely anonymous up to the UK border; this is no longer the case.

Because the transport environment is part of the public realm, it is one in which privacy and database protection are most vulnerable, and the development of cheap and available technology is a significant threat.

Surveillance by legitimate public authorities compromises privacy, but not as much as illegitimate surveillance or the private abuse of personal data databases. Government should concentrate on facilitating more sharing of data among legitimate authorities, while cracking down on unnecessary release and other abuses.

April 2007

APPENDIX 14

Memorandum submitted by Symantec

1. Symantec welcomes the opportunity to submit evidence to the Home Affairs Select Committee on issues relating to the growth of, and public concerns regarding, public and private databases and forms of surveillance.

Executive Summary

2. The pervasive nature of advanced technology has lead to the internet, mobile telephony and communication technology becoming a part of our everyday lives. In this era of technological development, data is the currency of the age. As the network economy continues to grow the amount of personal information being processed, accessed, shared and stored online looks only likely to increase. The development of innovative online services and the future delivery of public services will rely on individuals continued willingness and trust to share information online. Therefore addressing citizens concerns over data security is essential to allay public fears, realise the full benefits and opportunities provided by technology and increase citizens' confidence in the online connected world.

3. It is important to recognise however, that data has been collected and surveillance conducted long before the emergence of the database, Internet, mobile telephony or even CCTV. Information communication technology has not caused surveillance to occur. Rather technology is simply a tool that has become prevalent in our everyday lives and has lead to an increase in the provision of goods and services electronically which requires the sharing of information. It could be argued that it is not so much a surveillant society that is emerging but rather a pervasive computing environment within which increased importance must be placed on the responsibility of industry, government and also citizens to protect their personal information.

4. In this era of transformational government and online public service delivery an increase in the use of technology is resulting in online data collection and sharing. It is suggested that the introduction of performance related standards and an annual scorecard for government IT systems effectiveness could act as important incentives for departments to introduce effective, efficient and measurable data management and data privacy controls.

5. In addition greater understanding and awareness is needed by citizens on the role of existing effective legislation in place to protect data from misuse such as the Data Protection Act. Symantec also believe consideration should be given to the introduction of a data breach notification law currently being considered by the EU. Raising understanding of the positive benefits of database management and technology in protecting information could also have a positive impact on citizen's fears over the power and role of database technology. In particular raising awareness of how the creation of formalised, structured databases can increase the security of data and protect information against unauthorised access and possible misuse.

Access by Public Agencies to Private Databases

6. Formalised data sharing gateways between the public and private sector enable information to be assessed against data stored on existing databases within a legally agreed framework. Symantec recognise that there are public concerns over the use of data sharing gateways. For example while consumers consent to checks on their identity being conducted when applying for financial services, when similar checks are conducted by public agencies this is regarded as intrusive and leads to privacy fears. Public concern may derive from the fact that while financial organisations require an individual's consent before checks can occur, no such consent is required in a data gateway investigation.

7. However, technological safeguards and legal protection are in place can ensure the data provided through data sharing gateways is appropriate and relevant to the purpose for which the data is being sought.

8. Data management systems can ensure only the relevant and appropriate data is shared through the gateway. Having a structured approach to database management ensures that the data collected by an organization is caterogrised, stored and protected appropriately. Automated processes mean the relevant data allowed to be shared with a public agency is clearly defined and easily retrievable. This means that only the data legally allowed to be shared is accessed, meaning companies meet legal requirements whilst preventing unlawful processing or unauthorised sharing of data. The alternative to having a structured database solution in place is a fragmented approach where data is held on multiple operating systems, on multiple applications and increasingly across shared networks. This can lead to information being scattered across a number of different platforms or accessible by various partners, resulting in greater insecurity to valuable and sensitive personal information.

9. The Data Protection Act (DPA) is an important piece of legislation that outlines the legal requirements for the processing, privacy and disclosure of individual's data. It states that data held securely for one reason cannot be shared, or used, for another purpose. It can be suggested that citizen's fears regarding the privacy of their data may derive from a lack of awareness of their rights under the DPA and the efforts made by the private sector to adhere to these laws. It is suggested that educating citizens on the role of data sharing gateways and the DPA's principles could instill greater confidence and assurance in the role of the data sharing that currently occurs between the private and public sector.

Data-sharing between Government Departments and Agencies

10. Technology enabled transformation of government is a visionary strategy that will improve the quality, efficiency and cost effectiveness of public services. The take-up by citizens of e-government services will rely on having systems and processes in place that can ensure the confidentiality, integrity, availability and privacy of personal data shared with government. However, at the heart of the Transformational Government agenda is a shared services culture; one which will require greater data sharing between and within government departments.

11. Citizens' fears over data sharing by government departments presents a major challenge to the future delivery of public services. However having systems in place that can ensure access to particular types of data is only granted to appropriate and authorised individuals in the relevant departments or agencies will be a key factor in preventing unauthorised access to sensitive personal data.

12. Standard policies, procedures and requirements for data management means access levels can be allocated to particular types and levels of data by government departments and bodies. For example the introduction of common access controls across the NHS IT systems could ensure only designated NHS personnel have the right to access patients sensitive information; reassuring citizens that their data is not vulnerable to unauthorized access or misuse. The access given to NHS staff could be monitored and audit trails produced, providing additional reassurance to patients that the confidentially of their data is being maintained. Access levels can also be used to dictate the information that can be shared outside an organization for example to another NHS body or even to an insurance company's private database.

13. Another example of this approach is the new Management of Police Information (MOPI) database; part of the Impact program which is aimed at improving the way UK police forces manage and share information. It is understood that MOPI will introduce standard procedures to ensure only authorised personnel can obtain and record information on the system. In addition rules for authorised sharing of information among police services and agencies will also be put in place which all forces will be required to implement and follow by December 2010.

14. However, MOPI is currently one of many projects being developed that focus on the need to co-ordinate data across multiple criminal justice organisations. As we move forward Symantec believe, where possible, consideration should be given to how these information related projects might be brought together. This would ensure projects do not become isolated and create duplicate databases and procedures for access to information which could challenge the standardised approach being implemented under MOPI.

15. The introduction of effective access levels across all government departments would require common data management procedures and practices to be developed and implemented. The latest version of the CSIA eGovernment framework for information assurance introduces much needed guidelines on the standardisation of processes, terminology and procedures for the secure access, authentication and management of data within and across government departments; essential as the development of automation and reliance on shared services increases. The framework document provides government departments with the information needed to take a proactive approach to protecting information assets, understand their duties and responsibilities for ensuring the systems underpinning online services are secure and above all how to implement existing best practice in Information Assurance. Symantec believes that trust in electronic services is best achieved through Information Assurance and welcomes the approach being taken by the CSIA.

Existing Safeguards for Data Use and Whether They are Strong Enough

16. The European Commission is currently conducting a Review of the EU regulatory framework for electronic communications networks and services. As part of this review amendments to legislation are being considered to require network operators and Internet Service Providers (ISPs) to notify customers, and national regulatory authorities, when a security breach has occurred leading to the loss, alteration, and unauthorized disclosure and access of data. Symantec has welcomed the requirements proposed which would introduce an important incentive for ISPs to increase the safeguards and levels of security for data stored online.

17. A data breach notification law could help raise greater awareness, reassurance and trust amongst individuals on how their personal data is protected on-line and what recourse they may have in case that data is disclosed without authorisation. Symantec believes that the scope of the data breach notification should not be limited just to ISPs and electronic communication service providers but to all sectors that process sensitive personal information on-line. For example this could include retailers and financial institutions.

18. When considering the introduction of a data breach requirement however, it will be important to define the breadth of the disclosure requirements and also ensure providers that take adequate steps to protect data and suffer a breach are not held liable. It will be important to determine whether information on a breach that has occurred should be reported on a confidential basis or circulated publicly. For example, breach information could be given to the National Regulatory Agency (the Information Commissioner's Office in the UK) which could then disseminate relevant information to the public. Alternatively information could be openly disclosed to all those individuals involved. Given the possible negative impact on users' confidence in both public and private sector online services, the issue around the confidentially of data breach information is an area that will require further consideration and discussion going forward.

19. Finally ensuring that electronic communication service providers that have demonstrated adequate levels of security, but do suffer a data breach, are relieved from liability for the breach will be important also. As it would act as an important incentive for providers to ensure security measures are kept up to date and can protect data at the required levels.

The Monitoring of Abuses

20. Real time monitoring of databases for possible abuses may invoke connotations of a survellant society. However, it is an example of how technology enabled surveillance can protect individual's personal information. Monitoring technology provides automated analysis of databases which can provide alerts to unauthorised activity such as access to sensitive data or intrusion from an unknown source. The use of such technology can ensure abuses of information are identified and dealt with quickly and effectively.

21. Having in place effective oversight mechanisms for the legislation and regulation relating to the use of data is important for ensuring those involved are held accountable and sufficient penalties for misuse of data exist. The Information Commissioners Office plays a vital role in ensuring the legislation for the privacy of data in the UK are enforced, abuses identified and prosecuted accordingly. However, Symantec believe an urgent review of the Information Commissioner's Office powers is required in order to remove any existing limitations on the ICO's ability to investigate possible misuse of data and increase the legal and financial penalties for offences. Consideration should also be given to the staff and resources currently allocated to the Information Commissioner to ensure the ICO's continued effectiveness.

Potential Abuse of Private Databases by Criminals

22. Data is one the most important assets of any organization and a valuable target for attackers. Identity related information is becoming a valuable asset to criminals, resulting in both public and private sector databases containing sensitive information increasingly vulnerable to attack.

23. According to the latest Symantec Internet Security Report, between July and December 2006 the government sector was the highest for data breaches, accounting for 25% of all breaches leading to the loss of identity related information. The report found that 28% of these breaches were caused by insecure policy such as a failure to develop, implement, and comply with an adequate security policy. It can therefore be suggested that most breaches of this type are avoidable.

24. The Symantec report identified the development of malicious computer code and programs designed specifically to expose confidential information. These threats can expose sensitive data such as confidential data files and can also give a remote attacker complete control over a compromised computer. In the last six months of 2006, threats to confidential information made up 66% of the volume of top 50 malicious code reported to Symantec; an increase over the 48% reported in the first half of 2006. Threats that allowed remote access, such as back doors, made up 84% of confidential information threats while keystroke logging threats made up 79% of all confidential information threats.

The Case for Introducing Privacy Impact Assessments

25. Regulatory Impact Assessments (RIAs) play an important role in providing an independent evaluation of the possible impact, side effects and costs involved in the introduction of proposed government legislation. The introduction of Privacy Impact Assessments (PIAs) is a suggestion that warrants further consideration and discussion. Having in place an opportunity for independent assessment of the possible impact of government legislation on the privacy of individuals data could be a useful tool for allaying public concerns over the safety of their information; particularly as we move towards an era of data sharing. However, further consideration would need to be given to the remit, scope and particular areas the PIA would consider when making an evaluation. For example, it would be important that PIA's take into consideration the existence of current technological tools and solutions available to address privacy or data security issues when assessing and determining if legislation should be introduced.

26. It is important that privacy concerns, which could be addressed by the development of innovative software solutions, should not be used as the sole argument for not introducing legislation. Further consideration should be given to how PIA's would be developed to ensure the use of PIA's does not inhibit competition or the development of diversity in the software industry to address data security and privacy concerns, or prevent data security solutions being developed to meet a particular requirement by either the public or private sector.

27. As we move forward with the transformational government agenda and increased data sharing consideration should also be given to assessing the ongoing effectiveness of government IT systems to protect individual's data. For example, in the United States the Federal Information Security Management Act (FISMA) mandates auditable procedures and policies to ensure the ongoing security of the IT systems used by US government departments and contract partners. Under FISMA government systems undergo regular monitoring and an annual audit resulting in each department receiving a grade which is published in an annual government scorecard.

28. The introduction of performance related standards and an annual scorecard outlining the ability and effectiveness of UK government IT systems to protect information, could act as an important incentive for departments to adopt effective policy management procedures, processes and controls that can assure data privacy and prove the quality of IT systems. Such a requirement could also drive those private sector partners connected to government systems to address their data security issues and implement effective data access and privacy measures.

Privacy-enhancing Technologies

29. The market offers a number of technologies solutions and tools suitable for different environments and different user-sophistication that can afford adequate level of security and protection for personal sensitive information. The information security industry continues to develop innovative solutions that can ensure the security and privacy of individual's information in the evolving threat landscape.

30. Easy to install and manage integrated security solutions are available that can provide critical security technological, such as firewall, content filtering, antivirus and intrusion detection. However, technology alone cannot be relied upon to protect information assets. Symantec believe a multi-layered approach to protect information assets is required that includes having appropriate technology in place, effective policies and procedures for data access and education and training on the importance of ensuring data security and privacy.

Profiling

31. In the current global competitive marketplace, being able to respond to customers needs, quickly and effectively is a key competitive advantage. Email and the internet are integral tools in enabling companies to communicate effectively with customers and customize the goods and services offered to individuals.

32. Customer Relationship Management (CRM) database systems enable firms to provide personalised, value-added services that meet consumers growing demands both quickly and effectively. The use of such systems however rely on individuals agreeing to personal information being processed, stored and shared online by giving their informed consent. While consumers may feel that the use of CRM's system to tailor information to consumer may be intrusive, the e-Privacy Regulations allows businesses to use an individual's personal information where there is an existing customer relationship to provide information on similar products.

33. By having in place an effective database structure enables companies to comply with requirements under the e-Privacy Regulations by sending information only to customers that have provided their consent. It can be suggested that individuals will only be receiving information from legitimate firms because they have provided their consent but may have simply forgotten. Individuals also have a responsibility to ensure that their data is shared appropriately and securely with online partners.

About Symantec

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, California. Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com.

April 2007

APPENDIX 15

Memorandum submitted by the Surveillance Studies Network

Authors

Dr Kirstie Ball, Senior Lecturer in Organisation Studies at the Open University Business School, 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.

Professor Clive Norris, Professor of Sociology and Deputy Director of the Centre for Criminological Research, University of Sheffield, UK.

On behalf of the Surveillance Studies Network

The Surveillance Studies Network is a charitable company, registered with the UK Charities Commission, dedicated to public education on the subject of surveillance. For more information, please contact the Corresponding Author.

Executive Summary

1. The Surveillance Studies Network welcomes this inquiry and the opportunity for high level debate on the surveillance society that it offers. We make nine observations on issues that we feel the committee should consider.

2. Dataveillance. Searchable and remotely accessible databases are increasingly being linked together allowing for three operations to be performed: profiling, social sorting and pre-emptive categorisation.

3. Targeted and Mass Surveillance. The re-emergence of mass surveillance poses particular problems for several long-standing presumptions in law: Habeus Corpus, The Presumption of Innocence; Reasonable Suspicion; and The Right to Silence.

4. Data Quality. If judgements are increasingly made on the basis of profiles in databases, then the quality of the data needs to be very high, however combining databases can allow low-grade data to circulate more widely.

5. Technology. There is a significant gap between the dreams of Joined-Up Government and the reality afforded by technologies, with contracts awarded without proper trials, and a mistaken but increasing assumption that if something is technically possible then it is good policy.

6. Blurring of Public and Private Boundaries. State and Private sector are increasingly bound together in surveillance practices, with important implications for data protection and privacy.

7. Public Awareness, Consent and Trust. The public have a strong interest in individual rights, and the two things should not be played off against each other. Consent needs to be rethought with the constant circulation of data. However oHoweverHknowledge of technology and policy issues is low, as are levels of trust in institutions.

8. Privacy. Data protection is inadequate for protecting the privacy of the citizen, and the concept of privacy should be strengthened in British law. However privacy may be inadequate as basis for rights in the surveillance society.

9. Personal Information Economies. Privacy Enhancing Technologies (PETs) cannot be regarded as a panacea, and if they become the main solution could lead to a society of privacy haves and have-nots.

10. The Regulator. The ICO needs greater resources and inspection capacities. However greater coordination and direction is needed at the EU level.

Introduction

1.1 As Directors of the Surveillance Studies Network and authors of the Report on the Surveillance Society for the Information Commissioner, we welcome the decision of the Home Affairs Committee to hold this inquiry, *A Surveillance Society?* We feel such a high level debate is long overdue and are pleased that our report has gone some way to initiating such a move.

1.2 The details of our arguments may be found in the full Report on the Surveillance Society, which we append. We are making a submission separate from the Information Commissioner as we believe there may be differences of emphasis, and the Committee would benefit from both of our perspectives.

1.3 We will outline ten areas which we believe are crucial for the Committee to consider: Dataveillance; Targeted and Mass Surveillance; Data Quality; Technology and Decision-Making; Blurring of Public and Private Boundaries; Public Awareness, Consent and Trust; Privacy; Personal Information Economies; The Role of the Regulator. The following paragraphs describe the issues raised in these areas and pose questions pertinent thereto.

2. *Dataveillance*

2.1 Contemporary computer databases have added a distinctive dimension to information collection and surveillance in that they are both searchable and remotely accessible.

2.2 Such databases are increasingly being linked together either directly or through information-sharing practices.

2.3 The distinctive qualities of these databases allow for three operations to be performed that change the nature of the relationship between the organisation conducting surveillance and those surveilled: profiling, social sorting and pre-emptive categorisation.

2.3.1 Profiling, the creation of detailed files of personal information matched from multiple sources, allows for a virtual person (data-double or data-shadow) to be created within the database. What are the material consequences of profiling for individuals, groups and society?

2.3.2 Profiling has consequences for the individual in terms of their entitlements and life chances. However, when aggregated, profiles have the potential to extend, intensify and exaggerate existing social distinctions and divisions, or to create new social categories. The potentially serious consequences for life chances need to be documented and explored, whether or not any criminal matters are involved, especially if such operations are automated.

2.3.3 Of particular concern is the movement to pre-emptive categorisation, where individuals or groups deemed by virtue of their profiling as "dangerous", "risky" or even simply uncertain or unknown, are targeted for intervention in advance of any crime having been committed. How much is this already occurring and how does it affect the operation of law?

3. *Targeted and mass surveillance*

3.1 It is important in this context to make the distinction between targeted surveillance 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) poses particular problems for the operation of the law in democratic countries like the UK.

3.2 Several long-standing presumptions are currently challenged in new ways, and no longer provide clear safeguards: *Habeus Corpus*, The Presumption of Innocence; Reasonable Suspicion; and The Right to Silence.

3.2.1 *Habeus Corpus*. Is the right to the body of the individual challenged through mass implementation of fingerprinting, DNA and drug-testing, by police and for other proposed identification purposes, and the retention of the results of such tests? There are also significant questions as to the status of the data-double in relation to the body. If such a corpus of information is increasingly as important for life chances as the physical body, is there are need not only for a re-statement of *Habeus Corpus* in relation to the conventional body, but also its extension?

3.2.2 The Presumption of Innocence. Does the widespread collection and keeping of evidence and the operation of pre-emptive categorisation mean that the traditional presumption of innocence is in danger of being turned upside-down? The increasing use of "Orders" (Control Orders, ASBOs etc) seems to be of particular concern: to be instituted, these orders require no proof of criminal activity, yet breaking them is a crime.

3.2.3 Reasonable Suspicion. Similarly, does the collection and retention of evidence from all those arrested constitute an erosion of the principle of reasonable suspicion, in favour of indiscriminate mass surveillance?

3.2.4 The Right to Silence. What are the implications of the right to silence in a state which seems increasingly to regard citizens as needing to prove their bona fides or face the consequences?

4. *Data quality*

4.1 If judgements are increasingly made on the basis of profiles in databases, then the quality of the data would have to be unimpeachable.

4.2 Unfortunately this is not the case. In particular, when national and local databases are combined, low-grade intelligence can begin to circulate more widely and acquire a reliability it does not deserve. Examples have included the DVLC and Criminal Records, and potentially Connecting for Health programme and others.

4.3 What can be done to remedy this? Certainly, there needs to be a change in culture and more awareness of the poor quality of much data already in databases.

5. *Technology and decision-making*

5.1 It has to be recognised too that there is a significant gap between the dreams of Joined-Up Government and the reality afforded by technologies. Technological systems have organisational, cultural, and technical limitations: there have been many examples of the failure, limited performance or massive cost or time-overruns of state computerisation projects.

5.2 In particular, there is tendency to regard things as so urgent as to mandate the awarding of contracts for technological systems or their implementation before proper trials, tests or audits, for example the case of UK ID cards, or indeed facial recognition attached to CCTV.

5.3 The danger here is that the state may be seduced by commercial pressures and offers of "free" trials of systems. This is not just a question of speed but whether states are effectively subsidising the Research and Development budgets of private corporations (see also Section 6 below).

5.4 Does there need to be greater socio-technological knowledge amongst both ministers and civil servants, and training in how to assess both surveillance technologies in themselves and their possible effects directly, indirectly and in conjunction with other surveillance systems? It is also suggested that such knowledge and training might be independent of the security and surveillance industry.

5.5 It must also be recognised that there often should be limits placed on technologies. There is a tendency for the availability of certain technologies or the "needs of the system" to be used as reason for their use. However, because something can be done this does not mean that it should be done.

6. *Blurring of public and private boundaries*

6.1 The state makes increasing use of the private sector (through the Private Finance Initiative, Public-Private Partnerships and contracting out) to design and deliver public service interventions, even with regard to surveillance. Does the involvement of private organisations, with their own commercial interests, impact on the design and reliability of such systems and on the circulation of personal data?

6.2 In addition there is increasing pressure for the government to derive commercial benefit from the data it holds on citizens. Should such moves be possible with the existing framework of consent and data-protection laws?

7. *Public awareness, consent and trust*

7.1 Discussions of surveillance tend to oppose the interests of "public safety" against individual rights. However this is misleading. The public (citizens collectively) have a strong interest in individual rights, and the two things cannot be so readily played off against each other. In addition it cannot always be held that the state has the right to interpret the "public interest". What mechanisms would be needed to rebalance the debate in favour of the interests and rights of the citizen?

7.2 There is a key question as to the knowledge of citizens regarding the systems of surveillance to which they are subjected. In the current climate, it is clear that citizens have little knowledge or awareness of the surveillance systems to which they are subject, and indeed when they are so subject. They also have little knowledge as to the destination and use of the personal data which is collected by surveillance systems.

7.3 Hence, the question of consent must be addressed. If consent cannot be sought for every movement of data and every occasion on which data is used for purposes beyond that of its original collection, what can replace consent and what mechanisms would be used to enforce it?

7.4 Fundamentally, the question is one of trust: both trust of the citizen in the state, and of citizens in each other. What is needed for trust in a surveillance society? Could it be greater accountability and transparency on behalf of government? It would appear that if increasing amounts of data are to be sought

from citizens, that they should have a corresponding increased right first to know what is done with that data individually and collectively, to ensure its accuracy. and, second, to enjoy far greater rights of freedom of information and transparency of state institutions and surveillance systems.

8. *Privacy*

8.1 Data protection regimes are inadequate for protecting the privacy of the citizen, indeed the Data Protection Act does not mention the term.

8.2 Should the concept of privacy be strengthened in British law and what mechanisms would be needed for this?

8.3 Is individual privacy inadequate in itself as a right to deal with life in a surveillance society? Certainly ideas of collective or group privacy might extend the concept further, but what alternatives might there be? For example, in a surveillance society, one could make a case for a baseline assumption of transparency of citizens, private corporations and the state, moderated by specific exceptions.

9. *Personal Information Economies*

9.1 Privacy Enhancing Technologies (PETs) are increasingly used and will continue to be so used as the data-double increases in importance.

9.2 However, PETs cannot be regarded as a panacea. Do PETs represent simply a market response to problems of surveillance and privacy? If so, their spread and relative effectiveness will replicate social and economic divisions, leading to a society of privacy haves and have-nots.

9.3 Are we seeing the emergence of Personal Information Economies, where the wealthy will be able to manage their "data-double" and benefit from personal, consumer and state surveillance and technologically-enhanced privacy? In contrast, will the poor, marginalised and excluded, be increasingly subjected to both mass surveillance, categorisation and control without the means for the protection of their rights and freedoms?

9.4 In this context there must be a role of active regulation (see Section 10 below).

10. *The role of the regulator*

10.1 In our work for the Information Commissioner it became apparent that the ICO is not adequately equipped to watch state-commercial-citizen data-relationships in the surveillance society. This is through no fault of the ICO.

10.2 The ICO needs greater resources and particularly inspection or audit capacities with regards to government departments and agencies.

10.3 However it is unreasonable to expect the ICO to protect all the rights of citizens with regards to surveillance and privacy. So who can do this? In the absence of any convincing right of privacy in law, the British courts can do little, and perhaps this needs to be and EU-wide initiative. This would require greater work at the European level, perhaps in the form of a new Surveillance and Privacy directive, but this should also not be used as an excuse for not strengthening and extended the powers of the ICO.

April 2007

APPENDIX 16

Memorandum submitted by LGC Ltd

1. Executive Summary

1.1 The Select Committee has invited comment on a broad range of issues surrounding the "Surveillance society", following last year's report by the Information Commissioner. This response represents the views of LGC Ltd, one of the two main suppliers of expert forensic services to law enforcement agencies, regarding the handling of information associated with the operation of databases. This is primarily based around our experiences as one of the core suppliers of DNA profiles to the National DNA Database (NDNAD).

1.2 We recommend that, when databases are being planned, careful attention should be paid to the design of data flows to ensure that the data provided to individuals or organisations is the minimum necessary to permit them to perform their role within the overall process. In particular, only a limited number of authorised individuals at the core of a database should be able to link personal data to the individual concerned.

2. The National DNA Database Experience

2.1 There can be no doubt that the development of the NDNAD has provided a valuable tool to underpin the work of the police. The current system of operation embraces input from a range of DNA processing laboratories, including private sector laboratories, within a rigorously specified and assessed quality structure. This approach has brought all the benefits of competition into play, resulting in unit prices low enough to permit the routine application of DNA technology in volume crime and sample processing turn-round times measured in days or hours, rather than weeks or months. The effectiveness of the system is routinely demonstrated and is on a par with that of the national fingerprint and palmprint system "Ident1". As a result, the UK NDNAD is the envy of law enforcement agencies around the world.

2.2 The systems developed to support the operation of the NDNAD also provide a model for the development of other databases to support UK law enforcement. The transformation of the Home Office's DNA Expansion Programme into the Forensic Integration Strategy reflects the move to support additional forensic databases, such as a national footmark database, a National Ballistics Intelligence Database (NABID) and a National Injuries Database.

2.3 However, there is operational experience which has arisen over the life of the NDNAD which should be taken into consideration as additional databases are developed. In particular, there are issues surrounding the transfer and security of data and samples where we think that appropriate design of future systems could minimise the potential risk of inappropriate access to or use of information.

3. Oversight of the NDNAD

3.1 When the NDNAD was originally established in 1995, there was only a single authorised supplier of profiles, the Forensic Science Service (FSS), which was at that time a Government agency. The single suppler was unable to cope with the demand for sample processing and backlogs rapidly built up, to the point where turn-round times were in excess of six months. When a newly-privatised LGC offered to invest to provide additional processing facilities in 1996, a set of authorisation criteria for potential suppliers of profiles was developed by the FSS, including accreditation and proficiency testing requirements. Once LGC was able to offer its services to police forces, the processing capacity available expanded, turn-round times rapidly fell and the benefits of a competitive market began to become apparent. Other suppliers have subsequently been authorised to submit profiles to the NDNAD.

3.2 The role of "Custodian of the NDNAD" was created to safeguard the integrity of the Database, including setting standards for suppliers of profiles. Initially, this role was associated with the NDNAD within the FSS but, as the status of the FSS changed from a Government Agency to a Trading Fund and then to a Government-owned Company, this led to increasing tensions as other suppliers came to regard the FSS as being in an ambiguous, and privileged, position, as they were effectively regulating a market in which they were also competing as a service supplier. The Custodian role has therefore been separated from the FSS, and now sits within the newly-created National Policing Improvement Agency (NPIA). Although the FSS continues to provide some key supporting services to the NDNAD, such as IT support, the separation of roles is essentially complete, and the FSS is one supplier among others, all providing profiling services to the NDNAD within a closely regulated quality and security structure.

3.3 The structure which has evolved therefore consists of a range of quality-accredited suppliers profiling samples on behalf of police customers, with profiles being submitted to a central Database, and the resulting "matches" being sent by the Database back to the police forces.

3.4 Where there have been attempts to establish within a single commercial organisation other databases which were unarguably national in nature, as was initially the case with both the footmark and the Ballistic Intelligence databases, it rapidly became apparent that this was both commercially and strategically inappropriate, and that the NDNAD model was preferable.

3.5 We feel that the model that has been achieved, with an independent Custodian within Government setting standards for, and overseeing the operation of, a range of service suppliers from both the public and private sectors, represents an extremely effective system for operating a national database structure.

4. NDNAD Subject Sample Processing

4.1 In the case of samples collected from individuals for processing for addition to the NDNAD, the current system involves a police force submitting a DNA sample, typically in the form of a mouth swab, to the processing laboratory, together with a card carrying details of the donor. Both the sample and the card carry an unique bar-code number. The card also carries a numerical link to any associated Police National Computer entry (the "arrest/summons number" or ASN) as well as details of the donor, including name, date of birth, ethnic appearance and the type of offence involved.

4.2 In addition to processing the sample and submitting the resulting DNA profile to the NDNAD, the laboratory is required to capture some of the data from the card to submit to the NDNAD with the profile and to store both the residual sample and the card. This means that each processing laboratory holds a store of samples of individuals' DNA and a store of data about the individuals.

5. Too Much Information?

5.1 The laboratories do not need all of the data about the donor which is provided to them in order to be able to process the samples. The unique (and anonymous) barcode should be sufficient to identify the sample and to link the profile produced to the sample and therefore to the individual donor. In practice, it is accepted that any system involving large-scale sample and data collection and transfer can be prone to error, such as occasional inadvertent "sample swaps", so some additional data is of value in case it is necessary to resolve a discrepancy. However, this could be limited to a less specific identifier than a donor's name, for example a date of birth.

5.2 The residual samples are retained in case rework is required, including reprocessing for quality assurance. The ability to re-profile samples is of undisputed value, but storage of samples, containing the full DNA of donors, has raised issues of security, access and approval for use.

6. Managing the Data

6.1 The data-related issue which emerges is how the flow of sample-related data is managed, that is, which parts of the overall data held on an individual are required by each organisation within the data handling chain. Although all the data gathered during the processing of DNA subject samples is necessary at some point, not all data is required by all participants in the process. There is therefore a case for a "data audit" when establishing the flow of data to underpin a database, to review which aspects of the overall data needs to pass to and/or be held by each organisation involved. This contrasts with a "one size fits all" approach, involving access to a data package containing all the data required by all participants, so that each organisation within the data-handling chain can abstract the data they need.

6.2 We consider that, as the total amount of data held on individuals increases, this should not automatically be passed from one agency to another as a bundle to be "mined" by the receiving agency for the aspects that they require. There should instead be an effort to pre-screen data flows on a "need to know" basis, so that the total information available at each location is minimised.

6.3 The presumption should be that only those data points which are necessary for them are disclosed to each participant in the chain. In particular, the identity of the individual involved should ideally be encoded in such a way that those engaged in sample or data processing are not aware of the identity of the individual and only those authorised staff at the operational centre of, for example, law enforcement are in a position to link the various components of the data to the individual concerned.

6.4 Similarly, where samples are involved which potentially contain additional information about the donor, access will be required by processing organisations when they conduct their work, but any long-term storage should be undertaken only in closely-controlled repositories, to minimise the potential for unauthorised access.

7. Summary

7.1 Efficient construction and operation of databases will usually require the involvement of a variety of organisations, from within Government and the private sector. In addition to the usual arrangement for security vetting the individuals with access to data, any potential for "leakage" of information can be minimised by careful attention to the design of data flows and, in particular, by ensuring that only a limited number of authorised individuals at the core of the Database are able to link data back to the individual concerned. Although some details of its operations are still subject to debate, the National DNA Database has evolved to a position where it can offer a valuable model for the design and construction of future databases holding information about individuals.

April 2007

APPENDIX 17

Memorandum submitted by The Royal Academy of Engineering

Introduction

1. The Royal Academy of Engineering published its report *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* on 26 March 2007. That report covers many of the issues of interest to this inquiry. The following response takes some of the points made in the report and applies them to the specific issues that the inquiry addresses. One of the main themes of the report is that there is often a trade-off between protecting personal information and achieving greater levels of security and convenience. The need to strike a satisfactory balance is key and the view of The Royal Academy of Engineering is that this

balance is achievable, as long as IT projects that include the collection and processing of large amounts of data are properly designed and implemented. This will involve a focus on designing for privacy and thoroughly assessing and managing the risks in any system that will involve the processing of personal data.

Data-sharing Between Government Departments and Agencies

2. It is clear that greater data sharing could help to reduce fraud, and should make the delivery of public services more efficient. The current provisions for sharing and cross-checking data between government departments certainly stand in need of improvement.

3. However, greater data sharing brings with it increased potential for intrusion into peoples' lives and infringement of their privacy. People occupy many roles and, in principle, it should always be possible for an individual to keep these roles separate. For example, they may not want their employer to know personal information about their current or past health, or they may not want their employment history known to their doctor and so on. The more that information about the different parts of an individual's life is linked together, the more full a picture of them is created—revealing their history, their day-to-day activities and their general behaviour. The more a full picture of them is available, the more restricted the personal privacy they can enjoy and control.

4. Because data sharing can have such a significant impact on privacy, it should only carried out when there is an explicit need and reason. This could be to investigate benefit fraud, to compare and check health and social services records over time or for other important reasons relating to crime prevention and personal welfare. Data sharing should be made easier in order to support such justifiable and auditable purposes, but it should not be allowed to become routine.

Access by Public Agencies to Private Databases

5. If individuals' data are recorded on a database for a given purpose and with their consent, then that data should not be used for other purposes for which they have not given consent. This means that, in general, public agencies should not be allowed access to private databases. However, if there is need for public agencies to access private databases in order to investigate crime—for example, the Serious Organised Crime Agency accessing customer databases of financial organisations to potential cases of fraud—then there can be a justification for allowing access to those databases. However, there must be good reason for allowing that access, in the form of significant reason for suspicion of fraud or other financial crime.

Existing Safeguards for Data Use and Whether They are Strong Enough

6. Data collection and processing is currently governed by the Data Protection Act 1998 (DPA) which is enforced by the Information Commissioner. In order to be an effective force and to present a real deterrent against the misuse or reckless use of personal data, there need to be some changes to the DPA and to the role and powers of the Information Commissioner.

7. The Information Commissioner himself argues that the DPA is in need of clarification if it is to provide proper guidance and to be used to monitor data use. Many of the key terms in the Act, even including "personal information", are ill-defined (it is unclear in all cases exactly what counts as personal information and what does not), making the Act difficult to understand and adhere to. A keen eye should be kept on case law in this area for clarification of the concepts in the act and the rights that they entail.

8. However clear it is, the DPA can only deter misuse if there are appropriately punitive penalties for contravening it. The Information Commissioner has argued that tougher penalties are necessary to deter breaches of the DPA. In the report *What Price Privacy?* (May 2006), the Information Commissioner's Office (ICO) uncovered a black market for personal information. However, the report also showed that many of those individuals or organisations collecting and procuring personal information illegally faced only relatively small fines when taken to court.

9. Theft and misuse of individuals' personal data is a serious crime with damaging consequences. Penalties for abusing personal data should reflect the damage and distress that the crime causes. There is also need for tougher penalties due to the increased need to deter this sort of crime. Developments such as the Government's ID cards scheme, and the general moves toward "e-Government", will involve the collation of a wide range of detailed personal data about individuals—creating a honeypot for data thieves. Therefore, there must be more serious consequences for those who would be tempted to access this data fraudulently, in order to diminish its attractiveness. The Information Commissioner has argued for the need of tougher penalties including custodial sentences for illegal collection of personal data and The Royal Academy of Engineering supports this call.

10. The investigative powers of the ICO are limited in that its role is largely reactive: ie, action is taken only when a complaint is made. The ICO has no powers to carry out audits of information handlers without their consent. The lack of a threat of random checks may mean that many organisations are not as stringent as they would otherwise be in following the law. It would be of great benefit if the ICO could have the power to perform such audits, or to have such audits carried out on its behalf.

Potential Abuse of Private Databases by Criminals and the Monitoring of Abuses

11. There is always a risk of databases being abused by criminals, especially if they are connected to the internet. One way to diminish this risk is to follow some general principles for protecting the information on databases:

- Never store personal data in unencrypted form. If data are encrypted, the data remain secure, even if copied.
- The minimum amount of data should be kept for the minimum amount of time; this will reduce the likelihood of data being leaked, lost or misused.
- Personal data in large databases should be checked regularly with data subjects to ensure that they are accurate.
- If a database contains personal data about many people, or vulnerable people, the database access software should be developed to very high standards of security engineering. The necessary standards far exceed normal commercial software quality.
- If data are lost, individuals affected must be informed and compensated swiftly.

12. Encrypting data cannot guarantee their security as encryption codes can be cracked. However, encrypting data means that it is far harder to make use of leaked data and means that if data are stolen it will take a certain amount of time before they can be used. This extra time provides the opportunity to take action—for example, if bank details were stolen it would provide time to change those details before a criminal made use of the data. Encrypting data would also mean that they would be less attractive to opportunist theft, for example, database operatives being bribed for information.

13. For databases containing valuable or sensitive data, systems should be designed to keep an automatic audit of when the data are accessed and by whom and especially when data are changed. This can help to prevent individuals misusing or leaking data.

14. Personal data can be made vulnerable as a result of non-malicious mistakes as well as by criminal acts. This could be by disposing of personal information in an insecure way or through the loss of computing equipment with personal information stored on it. Although such actions are accidental, they are nevertheless negligent. The organisations responsible should be forced to recompense their clients if they make their personal data vulnerable—perhaps by having to write and apologise to each, offering compensation for the inconvenience of cancelling and replacing cards. Such penalties are used in California, serving to make onerous demands on those companies who are not careful with clients' data. The threat of having to go through such processes if customers' or associates' data are compromised should encourage organisations to be better custodians.

15. There should be a requirement for organisations holding personal information to store it according to the principles above, in order to minimise the possibility of the data being misused by criminals or made vulnerable by other means.

The Case for Introducing Privacy Impact Assessments

16. Privacy impact assessments (PIAs) may be useful in ensuring that government policies and their implementation do not infringe excessively on people's privacy. However, it is by no means certain that they will prove effective and they may well hinder the development of ICT projects. It is important to monitor the introduction of PIAs in Canada in order to assess whether PIAs are effective in protecting privacy and whether the extra bureaucracy is outweighed by the intended benefits.

Privacy-enhancing Technologies

17. Designing for privacy is essential in any large scale IT project. Basic strategies for protecting privacy include encrypting data, not retaining data unnecessarily and not retaining data for excessive periods of time. It is also essential that, in any large scale business change project, the need for a database of personal information is scrutinized closely. If that business change can be executed without collecting personal data then it should be carried out in that way.

18. The National ID card in particular would benefit greatly from being developed using privacy-enhancing technologies wherever possible. An ID card need not be developed on the model of a standard identity card with a photograph, name and other personal details on it which give away the identity of the user as soon as the card is presented. Rather, the identity card should be thought of in terms of the chip that holds electronic information. This chip is a small computer and can be used in a sophisticated way. For example, information on the chip can be partitioned so that it can be used to verify important information, such as nationality or age, without automatically revealing all of the other information that is stored on it. In this way the ID card can have the uses intended for it without it inevitably infringing people's privacy.

19. In general, there is a need for further research into privacy enhancing technologies and into designing for privacy. Designing for privacy needs to be introduced to technologists as a central component of their education and ongoing training so that incorporating privacy protecting measures into IT systems becomes as commonplace as incorporating safety measures in car design.

Profiling

20. Profiles are created to make predictions about people and their likely behaviour, and can be used in marketing, insurance, the health service and the financial sector. The problem is that the categorisation is rarely perfect and individuals may perform in a manner that puts them into a group without real justification—for example, coincidentally using a bank account in a manner that suggests criminal activity. Profiles may also be created automatically which group people together unfairly. Thus people may find themselves stigmatised as criminals or bad creditors, because of the profile that they are deemed to match. People should be made aware when the decisions about them are made on the basis of profiling methods, so that they can contest those decisions where appropriate.

21. Profiling can also be carried out in order to identify people as potential criminals, so that they can be closely monitored or included in the investigation of a crime. This might be done in relation to preventing and investigating terrorism in particular. There seems a *prima facie* argument for such profiling—namely that more time can be spent putting the people who fit the profile under extra scrutiny, and less can be spent on those who lie far outside it. Stereotypes do exist, and people may feel that it is a waste of resources to screen people who are nothing like the stereotype.

22. However, this tactic risks treating all people who fit a certain profile as potential terrorists or criminals. It is redolent of racism, ageism, sexism and discrimination against particular religions or denominations. It is very hard to accept that profiling along such lines should go on in a free, open and tolerant society. In addition, profiling in this manner may be counterproductive, since focus on one perceived threat may result in overlooking other threats. It may also generate distrust of the authorities that use such profiling methods—just as police bias towards certain ethnic minorities in making stop and search investigations can undermine trust in the police. While profiling might seem justifiable, its consequences undermine any justification for profiling methods.

CCTV

23. The UK has more surveillance cameras than any other country and the number of cameras in public spaces continues to grow. Surveillance of public places inevitably infringes on the privacy of law-abiding individuals and thus its proliferation stands in need of significant justification. However, evidence that CCTV is useful in preventing crime is very weak—it is often only effective in limited contexts (such as in car parks) and in conjunction with other measures (such as improved street lighting). The expansion of camera surveillance should be curbed until there is good evidence that it deters crime and terrorism. Furthermore, since modern cameras use digital images that can be stored indefinitely and searched electronically, there should be clear regulations on the retention and use of surveillance footage.

The National DNA Database

24. It is important that the national DNA database is used only to store the DNA profiles of those individuals involved in criminal proceedings and that the database does not expand into a comprehensive database of all people living in the UK. DNA samples and profiles should be collected only when there is good reason and, in the case of samples taken from volunteers, where there is explicit consent for the samples to be used for a given purpose. Samples and profiles should also only be retained when there is good reason or explicit consent—they should not be kept on the basis of the existence of a mere possibility of their being useful in detecting future crimes. If a volunteer offers to give a sample to help the investigation of a specified crime, this consent cannot be extended to the investigation of other crimes, past present or future, or other purposes.

April 2007

APPENDIX 18

Memorandum submitted by NO2ID

A. Introduction

This submission

1. This submission has been prepared by members of the national campaign against ID cards and the database state, NO2ID. Our volunteers study legislation and government proposals as well as near-government policies and technical developments as they appear, and endeavour to analyse their implications for a free society and individual liberty and privacy.

2. The inquiry has scope to begin to address NO2ID's concerns and we welcome it.

About NO2ID

3. 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 brings together individuals and organisations from all sections of the community and seeks to ensure that an informed case against state identity control is put forward in the media, in national institutions and among the public at large.

4. NO2ID is supported by parliamentarians of all parties and more than 100 organisations, including trades unions, political parties, local authorities and special interest groups have made formal statements supporting the campaign. More than 30,000 individuals have registered their support. We are funded by membership fees, occasional merchandise sales and fundraising events, as well as grants from the Joseph Rowntree Reform Trust Ltd, the Andrew Wainwright Reform Trust Ltd and individual and collective donations.

5. The campaign is staffed entirely by volunteers and we have a growing network of local groups across the UK, currently in as many as 100 towns and cities.

NO2ID's remit

6. NO2ID is neutral on most political questions, and non-partisan. 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.

7. We are not worried by data used in genuinely anonymised form, or in a statistical or collective manner for administrative or business planning or to make offers that can be refused or ignored. We hold that sophisticated market analysis techniques are not inherently intrusive, because they do not imply intervention in, or censure of, the lives and lifestyles of individuals.

8. On the other hand, 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.

B. General Remarks

9. The scope of the threat is, sad to say, much broader than the Home Office. Overspill into other departments is not merely incidental, as the terms of the inquiry might be taken to suggest. We believe that every select committee is potentially outflanked by a changing culture of government and changing methods that begin to evade scrutiny.

10. The creation of a surveillance state is inherent in the strategic conception of "Transformational Government", which 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" identifies the "barriers" to broad data sharing as human rights law, data protection, common law confidentiality, and the fundamental legal principle of *ultra vires*. NO2ID submits that if the culture of government is to regard those safeguards—which may yet be too weak—as problems, then something must be done about the culture of government.

11. Pending the abolition of all bounds to state power by Transformational Government, 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.

12. An example of deceptively broad drafting is in 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. Catch-all provisions include clause 8(2) of the UK Borders Bill which appears to grant the Secretary of State the power to use information gathered using very sweeping powers, for any purpose whatsoever. Steady extension (it is hard to see any diminution) of powers using secondary legislation can be seen in relation to the Regulation of Investigatory Powers Act 2000.

13. There is seldom a case made for the institution of broad data-sharing powers this way. It seems to be a matter of unconsidered administrative convenience in most cases. NO2ID would approach the problem from the other direction: information should not be stored or transmitted without good reason and limited purpose.

14. This area of public policy has developed rapidly and quietly, lacking not just a comprehensive legal framework, but even an adequate conceptual one available to most people. The promotion of the ID scheme has consistently blurred the distinction between authentication and identification, as if it doesn't matter. We urge not just the Home Affairs Committee, but all parliamentarians to take the question of the database state very seriously indeed.

C. Specific Questions Raised by the Committee

Access by public agencies to private databases

15. There is no reason to object to public agencies using private services on the same terms as private bodies, given proper protections in private databases. However, we are very concerned if either information not normally available on commercial terms is obtained without proper judicial oversight, warrant or court order, or if it is used for purposes other than those for which it was obtained, or if commercial datasets are combined with government ones in datamining exercises for government. The objections to using private data for government datamining are precisely the same as those in the following paragraph.

Data-sharing between government departments and agencies

16. In NO2ID's opinion this is the most significant threat to liberty we currently face. Our principal objection to the Identity Card Scheme is that it serves to enable the broadest data-sharing and data-matching across government. It is inherent in all such plans that information is used for purposes other than those for which it was given, which amounts to the requirement that citizens (and private corporations, too) give absolute discretion to government every time they provide information to it.

17. Government appears not to recognise that data-sharing and data-matching create problems of their own at any other than a technical level. We believe that it both radically increases the power of government over the citizen: information, direct oversight, being power; and that it creates the preconditions for 'suspicion by computer' in which an arbitrary match is interpreted as cause for government intervention. This is already seen in embryo in the activities of TV Licensing, which presumes everyone has a television unless proved otherwise, and will harry the occupants of any address with no licence attributed to it.

Existing safeguards for data use and whether they are strong enough

18. Such safeguards as currently exist are liable to be overridden arbitrarily by statute. The Children Act 2004, for example, casually set aside all rules of confidentiality or data protection in establishing the Information Sharing Index (now unfortunately known as Contact Point). Because information sharing effects cannot by definition be localised, each such provision causes leakage.

19. We consider that regulatory oversight and punitive regimes can never be sufficient. This is not just a question of quantity, though the present Information Commissioner's Office is clearly overloaded, and would have to be many times its present size to catch up with the burgeoning database culture. The nature of the dangers is not susceptible to *post-hoc* management by regulation. They are either secret abuse of data in individual cases or systemic failures arising from the unpredictable impact of over-broad powers. It is better to use structural institutional means to pre-empt and limit difficulties, than try to cope with the consequences.

The monitoring of abuses

20. NO2ID is of the opinion that monitoring abuses, while it might help assess the scope of problems, is generally going to be too late. It is very hard to dismantle systems once established, particularly in the public sector. Better prevent and minimise abuses—both by avoiding collecting and collating data unnecessarily, and by technical means to increase security—and to provide for proper redress for those affected.

21. Proper redress for victims of abuses is critical in creating an incentive for the design of good systems. Prescribing punishment for an abuser is of relatively little value if he doesn't believe he will get caught or if the gain is sufficiently attractive. Liability for the operators of databases directly to the victims of abuse is much more likely to be effective in prevention.

Potential abuse of private databases by criminals

22. All databases are potentially subject to abuse. The more comprehensive they are the greater potential for abuse. NO2ID is surprised, therefore, that the inquiry narrowly specifies private databases. Those cases that we are aware of involving threats to individuals other than financial loss arose out of misuse of public databases to obtain personal information. Private databases place direct value on the information involved, and can go out of business if they are not trustworthy, so have incentives to audit use carefully.

The case for introducing privacy impact assessments

23. We do not consider that this is likely to be of any value. Examination of the regulatory and race equality impact assessments that appear with existing legislation suggests that such exercises are uninformative and provide no brake on government. In some cases (notably that in 2004 for the then Identity Cards Bill) they are used to propagandise for the legislation rather than provide useful information. Unless any such assessment is carried out by a body independent of the department sponsoring the legislation, and in the light of clear definitions of privacy, it is hard to see what it could add at all.

Privacy-enhancing technologies

24. NO2ID naturally supports technology to increase privacy. We note that the principal enemy of privacy-enhancing technologies has always been government. Government objects to pseudonymous and anonymous transactions and fungible identities, often for quite legitimate reasons, but rather than designing taxation and law enforcement around new technology, or on an assessment of risk, it has chosen to scotch new technology, or at least has failed to aid its adoption. In particular government has been exceedingly hostile to the use of strong encryption in commercial and private contexts since it became publicly available, and comprehensively undermined its commercial use in the Electronic Commerce Regulations.

25. Government should remove barriers it has deliberately set up to distributed trust and encryption technology. It should be prepared, just as it is in the financial system, to be an issuer of sound certificates and "lender of last resort" in that it will underwrite digital identity for those lacking it otherwise—and then to stand back. 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 is backs changes hands. The same needs to be made "obviously" true for authentication transactions.

Profiling

26. NO2ID's attitude to profiling depends crucially on what is meant by "profiling". As indicated in our general remarks, we do not regard data-analysis for market segmentation or other statistical purposes as harmful. What is of great concern is patterns in data being used to determine the treatment of individuals. Creation of suspect- or watch-lists on the basis of associations or abstract models of behaviour is dangerous. It erodes the idea that individuals are responsible for their own actual conduct and free unless they transgress the law. We submit that any use of profiling that involves direct or indirect intervention by government agencies (or their proxies) in individual lives must be justified on a case-by-case basis, and that it should not be accrued or accumulated in any way. Being suspected should never in itself be ground for further suspicion.

D. Additional Questions

27. We would like to draw the committee's attention to two further causes for concern in the conduct of government.

28. Quasi-private databases: Official powers are being used to require private organisations to carry out surveillance on behalf of the authorities. This can be formal and explicit, as with telecoms data retention requirements, or, perhaps more disturbing, indirect as where licensing authorities make participation in a fingerprinting and ID scheme imposed on customers a condition of a liquor license.

29. Pseudo-voluntary processing: Whereas third party use of data without proper permission has largely died out in the private sector It is commonplace for forms for public purposes to waive data protection in effect, while being in practice impossible to decline to fill in. Committee members have an example to hand in the "security" forms for attendees at party conferences, where data is not limited to use for the event, but may be used for any police purpose.

E. NO2ID's Recomendations

30. This area is still not well understood. We recommend all involved in policy formation and scrutiny exercise skepticism with regard to claimed trade-offs between privacy and government efficiency. Modern communications and IT offer scope to improve efficiency while still maintaining segregation between separate agencies.

31. 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.

32. In addition consideration should be given to new personal privacy and information privity laws, giving direct redress for improper surveillance or sharing.

33. There should be a presumption against government data-sharing with case by case approval and external oversight whenever it is permitted.

34. We beg parliament to be vigilant against catch-all purposes and broad drafting.

35. Regulatory safeguards; rules, references, tribunals, appeals, are not likely to be sufficient. Institutional structures which make those in a position to prevent problems liable if they fail to do so are desirable.

36. A privacy impact assessment is unlikely to be of value, more a diversion of scrutiny.

37. Government should assist rather than attack private use of encryption technologies.

F. Further Information

This is a vast and growing topic. We will naturally provide what further information we can on request and witnesses if required.

April 2007

APPENDIX 19

Memorandum submitted by The Law Society of England and Wales

1. Introduction

1.1 The Law Society's interest in the topic of "surveillance" is a product of its (public interest) concern to ensure that a clear legal framework exists within which increasingly powerful and pervasive technologies of surveillance are deployed. We are also concerned about the practical—and financial—implications that certain surveillance initiatives (like Identity Cards and the retention of web and phone records) could have on our members and their clients.

1.2 The Information Commissioner has warned that the UK is now waking up to a surveillance society. It is therefore important to engage in as wide a debate as possible across the spectrum of interests—from law enforcement to individual privacy. It is one of the reasons the Society hosted a seminar entitled "Surveillance—Security or Intrusion" in November 2005 and which was attended by leading academics, campaigners, officials and the Home Office minister responsible for Identity Cards.

2. The Nature of Surveillance

2.1 Surveillance today takes many forms. What is notable in recent years is that the growth and spread of digital technologies means that all of us nowadays leave a massive daily footprint of data—where we travelled and how (Oyster cards and automatic number plate recognition); who we telephoned and where we were at the time (mobile 'phone records); what we looked up on the Internet; who we e-mailed (communications data retention); and what we bought (credit, debit and loyalty cards). And all of this data is stored digitally and retained, sometimes for years.

2.2 A great deal of personal information that was formerly held in separate government databases is being joined together and the government has plans for more databases — like the National Identity Register—which will store even more. Moreover our images are recorded dozens of times a day on CCTV cameras and we are in the early stages of a national DNA database.

3. The Growth of Surveillance in the UK

3.1 Many people would argue that the level of surveillance is growing in all Western democracies. To a large extent this reflects increasing technological capability. In the UK the government has for many years been pursuing an ambitious programme to join-up its existing databases and develop new ones. Large private sector companies ranging from credit reference agencies to supermarkets and advertisers are also interested in gathering and processing large quantities of personal data. And, alongside the collection of data, the use of technologies like CCTV in public and private spaces is extremely high in the UK.

3.2 In deploying powerful surveillance technologies it is important to be clear about their purpose and to ensure that their use is regulated within a clear legal framework. It is usually a question of balance. Whilst the public may welcome increased data sharing between government departments in order to improve public sector efficiency they still want to know that the information they give to the tax authorities and their consultation with their doctor or their solicitor will remain properly protected.

3.3 Individual initiatives can no longer be considered in isolation. They need to be considered in terms of their potential contribution as a component of what the Information Commissioner has called "the infrastructure of a surveillance society".

4. Access by Public Agencies to Private Databases

4.1 There are real dangers in routine public sector use of private sector databases and in our view this should only occur without the consent of individual data subjects in exceptional circumstances (for example, serious crime or national security).

4.2 Amongst our concerns are:

- the quality of data on private databases;
- uncertain redress mechanisms for individuals disadvantaged by public sector use of incorrect or incomplete private sector data; and
- the inappropriateness of the public sector using databases that involve market-led judgments (for example about risk) that should have no place in public administration.

4.3 Government use of data held by large private sector data aggregators may effectively by-pass restrictions on the data that Parliament has agreed that Government can collect directly.

5. Data-sharing Between Government Departments and Agencies

5.1 Data sharing between government departments and agencies was the subject of a major government report in 2002 (*Privacy and data-sharing*, Performance and Innovation Unit, April 2002). The Prime Minister said that he wanted to see "early progress" in taking forward its recommendations. The following are amongst the recommendations that have not been implemented:

- the introduction of a Public Services Trust Charter setting out key commitments to citizens in protecting privacy and personal data in their interactions with public services and supported by service-specific statements;
- improved access for individuals to their personal data held by public authorities;
- better explanations of the individual's rights to access public data with clear points of contact;
- procedures to enable the public to correct their personal information with consideration of targets for response, monitoring and publishing performance data;
- access to quick and efficient procedures for dealing with complaints about the handling of personal information;
- all public sector organisations to have a named senior manager with clear responsibility for the handling of personal information;
- the development of methods for measuring data accuracy and reliability and an agreed set of methodologies for measuring and improving data quality; and
- internal and external audits across the public sector to improve data accuracy and reliability.

5.2 If data sharing between departments and agencies is to become more widespread (as part of "transformational government"), then these recommendations are worth revisiting.

5.3 We would also draw attention to the problem that widespread data sharing between departments and agencies will increase the risk of security breaches.

5.4 Finally, data sharing should support improved customer service (for example, automatic entitlement to benefits) and not just expenditure control. This may help to emphasise the importance of data quality to government since departments could be incurring expenditure on the presumption of accuracy and not just curtailing it. Such data accuracy would feed across into Home Office databases including the National Identity Register which, we understand, will make use of databases in the Department for Work and Pensions.

6. Existing Safeguards for Data Use and Whether They are Strong Enough

6.1 The European Data Protection Directive, the Data Protection Act, the Privacy and Electronic Communications Regulations, the Regulation of Investigatory Powers Act and the European Convention of Human Rights and the Human Rights Act do provide a robust legal framework that helps to safeguard individual privacy and personal data.

6.2 This basic framework is, however, quite complex and there is some evidence that it is not widely understood. Significant aspects of the basic framework are inevitably open to interpretation by the courts.

6.3 Statutory and regulatory additions to this basic framework, particularly in such areas as surveillance and retention and access to communications data, add an additional layer of complexity that makes the full picture extremely difficult to describe and understand. Vulnerable groups, for example groups whose first language is not English and who may be the target of police surveillance, may have particular difficulty. It is essential that the government ensures that appropriate levels of legal advice and support are available.

6.4 The interaction between the overall legal framework and the statutory and non-statutory data sharing gateways between department, agencies, local authorities and the private sector, appears to be opaque even to government.

6.5 The quality of administrative safeguards for data use appears to be unknown. Technical safeguards, apart from technical security safeguards, do not appear to exist.

7. Profiling

7.1 The problems flowing from the use of private databases, data-sharing and some lack of clarity in legal and technical safeguards are exacerbated where data is used for profiling.

7.2 Profiling in order to identify possible criminal activity is objectionable to the extent that it makes everyone a suspect. It is dangerous in its reliance on potentially inaccurate or out-of-context data and its use of unprovable algorithms. It tends towards a reversal of the normal burden of proof in both civil and criminal law.

7.3 Profiling may also take place secretly. Individuals may be treated differently or disadvantaged for reasons they are unaware of and do not have the opportunity to challenge. In the private sector this may involve individuals with high net worth receiving quicker, more personalised, service than others. This has no place in public administration.

8. The Monitoring of Abuses

8.1 There may be a good argument for giving the Information Commissioner additional powers and resources to monitor abuses in relation to the collection and use of data.

8.2 However, the numbers of databases and the detailed level of review required in order to identify abuses, may suggest that however well-resourced, no central organisation could adequately monitor abuse.

8.3 A requirement for independent data audits for government data bases and for private sector databases used by departments and agencies could be introduced. These could be made published annually. The Information Commissioner might undertake further investigation where departments or agencies failed an audit.

8.4 The case for rationalising wider oversight arrangement which currently include the Intelligence Services Commissioner, the Interception of Communications Commissioner, the Chief Surveillance Commissioner, the Information Tribunal, the Information (National Security) Tribunal and the Investigatory Powers Tribunal should be considered.

9. Conclusion

9.1 There needs to be a more thoroughgoing and informed public debate about what the right balance between security, efficiency and individual privacy should be. A review of the existing, labyrinthine, laws on surveillance and data sharing would be valuable and might lead to improvements to ensure that when mistakes are made, or when unwarranted intrusions into personal privacy occur, effective redress is available. It might also be appropriate to introduce mandatory administrative processes for properly assessing the impact on individual privacy of proposed initiatives.

9.2 Privacy Impact Assessments (PIAs) to be carried out as part of the legislative process could help to ensure a systematic approach to privacy questions. They might well involve multi-disciplinary expertise and we would anticipate that solicitors with relevant experience could play a significant part. If the outcome of the assessment was made public this would encourage welcome public debate.

April 2007

APPENDIX 20

Memorandum submitted by the British Computer Society

The British Computer Society (BCS) is pleased to send its response to the Home Affairs Committee, House of Commons, Inquiry on "A Surveillance Society?"

With almost 60,000 members, the BCS is the leading professional and learned society in IT and computing.

BCS is also responsible for setting standards for the IT profession. It is spearheading the IT in Professionalism programme and is also leading the change in the public perception and appreciation of the economic and social importance of professionally managed IT projects and programmes. In this capacity, the Society advises, informs and persuades industry and government on successful IT implementation.

BCS, as a Learned Society, also has direct responsibility for leading, encouraging, promoting, supporting and developing all aspects of teaching, research and technology transfer in the disciplines of, and relating to, computing, computer science and information systems.

BCS is determined to promote IT as the profession of the 21st century especially as IT is affecting every part of our lives. Therefore, BCS is pleased to take this opportunity to comment on such an important issue.

1. Scope

BCS has consulted its membership and particularly targeted its security experts—amongst whom a number are members of the BCS specialist Information Privacy Expert Panel (IPEP) and who have provided much input in to this consultation. (Information about IPEP is provided in the supplementary material at the rear of this memorandum).

2. Executive Summary

2.1 BCS is concerned about the amounts of data being collected about individuals, often without their knowledge, over a long period, how it is being collected and how it is being used—including, for example, selling data on to third parties.

2.2 There are serious concerns that if combined, this data can build up a comprehensive picture of an individual's life which can potentially be misused.

2.3 BCS suggests that government should build citizen-centric (rather than application-centric) multiple, distributed databases, aimed at minimising the amount of data collected and becoming more accurate.

2.4 BCS considers that a citizen's data belongs to that individual citizen and accountability mechanisms should be put in place to allow the citizen access to the data kept on them.

2.5 BCS continues to be very concerned about the security of the data being held as there is still little evidence that effective mechanisms are in place to ensure un-authorised access is not possible.

2.6 BCS would like to draw the committee's attention to the paper "Identity Myths and Identity Management". (See supplementary material).[160]

Comments

3. Access by Public Agencies to Private Databases

3.1 BCS members have expressed concern about the way in which information is being gathered eg schools taking children's fingerprints without reference to parents (http://education.independent.co.uk/news/article2434942.ece).

3.2 Members are concerned about the large amounts of (individually) low value information being collected over long periods that is (potentially) easily connected to an individual (unlike CCTV images) and built into a comprehensive picture of their life. Examples of such information include: mobile phone location records, Oyster card usage records, credit card transaction records, and indeed other telecommunications and Internet usage records.

4. Data-sharing Between Government Departments and Agencies

4.1 BCS believes it is necessary to recognise the difference between "data sharing" and "data aggregation". Instead of seeking informed consent to create links between existing databases, the government combines existing data into new databases; the NHS spine and National Identification Scheme are prime examples of this. In each case, a new, monolithic, legacy system is created.

4.2 Instead of this approach to combining data, we need to consider the federated approaches as currently being adopted by industry. The goal should be to create multiple, distributed databases, but with a minimisation of data such that each item exists only once (or in as few occurrences as possible). This will only be achieved by a fundamental rethink of government attitudes towards data ie:

- recognition that the data itself belongs to the citizen, **not** the state;
- building citizen-centric, rather than application-centric, systems; and
- aiming to minimise data and achieve greater accuracy, rather than the current approach of gathering as much data as possible.

4.3 Most importantly, we need to introduce accountability mechanisms that allow citizens to see what data has been stored, processed and shared and why. The Estonian ID Card model is an example of this.

[160] Not Printed.

5. Existing Safeguards for Data Use and Whether They are Strong Enough

5.1 BCS notes that there is very little guidance on what is considered adequate security for the classes of personal data. A blanket statement that conforming to an issued standard should be OK is not sufficient, especially where the standard is risk based and allows a wide range of attitudes to risk.

6. The Monitoring of Abuses

Note comments made in Sections 5.1 and 7.1.

7. Potential Abuse of Private Databases by Criminals

7.1 BCS continues to be concerned about data security issues relating, for example, to ensuring that un-authorized access to the data held on any widely assessable database(s) is not possible. This is a huge topic in which much work is being undertaken and yet there are still examples of successful un-authorised access being possible.

8. The Case for Introducing Privacy Impact Assessments

Risk basing for the type of security provision mentioned in 5.1 above makes the privacy impact assessment a good idea. BCS supports the introduction of mandatory (and published) privacy impact assessments for all government data sharing and government/ private sector data sharing.

9. Privacy-enhancing Technologies (PETs)

9.1 BCS would like to direct the Committee's attention to a vast literature on PET research which has developed. Some surveys of privacy-enhancing technologies which have already been carried out are listed below:

- http://www.ipc.on.ca/images/Resources/up-1bio—encryp.pdf
- www.cosic.esat.kuleuven.be/publications/article-835.pdf
- http://www.law.ed.ac.uk/ahrc/script-ed/vol3-1/mowbray.pdf

10. Profiling

10.1 Although BCS members can see the benefit of surveillance in many situations eg (hospitals, airports etc), there is a concern about the general tracking of citizens in their daily life since citizens are not in control of the data collection, post processing and potential profiling.

10.2 Of special concern at this time are vehicle tracking and DNA databases. Taken to its extreme, such information could be used as a tool of suppression by a police state.

11. ID Cards

11.1 BCS believes that the National Identification Scheme requires a fundamental re-think if it is to properly serve the needs of both the state and the citizen. We have, to date, witnessed a "binary" approach by government that assumes that:

- it is the responsibility of the state to provide authoritative identity data on citizens;
- an identity is either trusted or not trusted, with no tolerance in between; and
- private organisation will depend upon government—supply identification data, even where there is no liability upon government if that data proves to be false.

11.2 The role of government is not to identify citizens in any context except for travel documents. It is, twofold:

- to confirm *uniqueness* of each individual: that is to provide assurance that an individual has not claimed duplicate identities in order to exist as more than one entity. Note that this does not prevent the use of pseudonyms, since the individual may use as many names as they wish so long as they exist only once within the National identification Register (NIR).
- To confirm *eligibility* of the individual to exit with the NlR. This is not the same as identifying the individual. Once enrolled, a separate database may provide an audit trail of the enrolment, but personally identifiable information should not be required.

11.3 The existence of such a "National Uniqueness Register" would permit private organisations to build their own identification systems, with assurance that individuals cannot engage in multiple enrolments and hence claim false entitlement. Corporate uptake of identification services would be greatly accelerated. Furthermore, individuals would be far more likely to trust an approach such as this that minimises data gathering and hence the risk of misuse or modification of personal data.

12. Concluding Remarks

12.1 A wide-ranging enquiry, such as has been described in the announcement for this present one, can only produce general answers. BCS believes that the ground rules for security are already well documented and understood by government IT professionals. BCS anticipates that a general enquiry by MPs exploring 'large strategic issues' will elicit very little which is new and of value. This will result in the press picking up again on some of the identified risks and accuse the IT industry of incompetence once more.

12.2 BCS recommends that Committee members first clarify what they want to do and what specific outcomes (level of security/risk) they want to achieve under particular legislation. MPs have the duty of ensuring that all legislative changes are checked in detail for security/risk before they are approved.

12.3 Only at this stage, will it be appropriate for the BCS to comment on the critical *technical* aspects of legislative changes. We would also be very happy to provide further detailed input on the implications of proposed changes to the technical environment or business requirements, as and when the committee feels it to be appropriate.

Dr M G Rodd,
Director of External Relations at the British Computer Society (BCS)

April 2007

Supplementary Material

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.

This may include, but is not necessarily limited to, issues arising from privacy, data protection, data sharing, identity, freedom of information and digital right management. It reports to the Security Forum Strategic Panel and has a particular responsibility for the identification and addressing of information privacy issues within the Society and the wider community.

IPEP's members are selected to represent a broad spectrum of expertise across a range of industries, and include technologists, lawyers and privacy practitioners from academia, industry, service provision, healthcare and government sectors. The panel provides both formal input and informal advice to BCS policy, and contributes to policy of government and relevant non-government organizations.

IPEP has previously contributed to debates on national identity cards and transformational government proposals, and is currently considering issues as diverse as privacy of healthcare records, IT project management processes and data sharing initiatives.

APPENDIX 21

Memorandum submitted by Hewlett-Packard Laboratories

Executive Summary

Attainment of the Government's vision regarding digital services is threatened by many individuals' concerns over the increased potential for surveillance, over them and their actions, that consuming such services would offer. Adoption of digital service delivery infrastructures whose designs avoid the need to know the absolute identity of the service consumer would significantly reduce that potential and the concerns it creates. The technologies that are needed in such designs exist today and are available for use. Clear support by the Government for such system designs would provide the necessary catalyst to enable their widespread deployment. In turn, this would reduce the threat to attainment of that vision.

Introduction

1. Hewlett-Packard strongly supports the Government's vision of:

> "*Creating a country at ease in the digital world, where all have the confidence to access the new and innovative services that are emerging, whether delivered by computer, mobile phone, digital television or any other device, and where we can do so in a safe environment.*"[161]

It is clear that for the desired confidence and feeling of ease to exist, all consumers of such services must not only do so in a safe environment, but must regard that environment as safe. In turn, such positive regard requires that their concerns about being the subject of surveillance, whether based on actual experience of being the subject of surveillance, reported experiences of others or just a personal desire to enjoy their human right of privacy,[162] be addressed and resolved.

2. As the corporate research laboratory of Hewlett-Packard, we wish to submit comments to help the Committee to understand the potential role of information technology to address the privacy and trust concerns that many citizens have about surveillance. The scope of our comments includes the roles of privacy-enhancing technologies and trusted computing technologies, and the necessary rooting of their use in the human/social concept of trust.

Implications of Surveillance

3. Where the intent of surveillance, whether by government/public agencies or others, is for a clear and specific purpose that is generally viewed positively and the attainment of which is seen to be aided efficiently by surveillance, and the actuality is absolutely limited to that intent, it is to be expected that few would object thereto. However, unless all concerned with the instigating, sponsoring and operating surveillance have both met those criteria and been seen to meet them, this lack raises concerns in individuals, which in turn influence their behaviour. Scaling this argument up from individuals to society as a whole, it can be seen that attainment of the Government's vision will be affected by the feelings that individuals *en masse* have about surveillance.

4. Applying the above logic to the online world, it is clear that surveillance can be performed by a number of parties on both the actions of digital service consumers and on static information about them. The lack of precision, clarity and stability in Government statements about the specific purposes, operational details, controls and limitations over uses of personal data, etc. of schemes such as the retention of communications traffic data, the National Identity Register and Cards, the National DNA Database, the NHS database and various child-oriented services and databases (eg Connexions, the Electronic Social Care Record) does not provide assurance that any surveillance by government/public agencies would be exclusively of the acceptable nature referred to in paragraph 3. The same statement can be made about private sector providers of digital services, many of whom appear to pay minimal regard to the spirit, if not the letter, of the data protection regulations' requirements regarding their privacy policies. We therefore look next at some work we have done which provides an insight into the feelings aroused in individuals by the possibility of negatively-viewed surveillance.

The Individual's Viewpoint

5. A research project, named Trustguide,[163] was undertaken over a period of 15 months to October 2006 by HP and BT, sponsored in part by the DTI Sciencewise[164] programme. It took the form of workshops which explored the opinions of, in total, approximately 250 citizens with a wide mix of backgrounds, ages, interests and personal values, regarding the tensions in the provision of internet enabling technologies that also fulfil personal expectations of trust, privacy and security.

6. It is not our intention here to describe or summarise all the findings from this project,[165] but we wish to highlight the following findings that are relevant to the purpose of this submission:

- Lack of control and openness leads to mistrust. Citizens want more responsibility to be taken by government, the banks and ISPs (Internet Service Provider) and guarantees to be provided.
- Virtually all participants commonly referred to "risk" rather than "trust" when describing their ICT mediated experiences, and felt more comfortable and secure when restitution existed.
- A majority of participants believe that it is impossible to guarantee that electronic transactions or electronically held data can be secure from increasingly innovative forms of attack.

[161] March 2005 Connecting the UK: the Digital Strategy. Cabinet Office, Prime Minister's Strategy Unit, joint report with the Department of Trade and Industry.
[162] Article 8, European Convention on Human Rights.
[163] Trustguide website: http://www.trustguide.org.uk
[164] Sciencewise website: http://www.sciencewise.org.uk
[165] The Trustguide Final Report is available at http://www.trustguide.org.uk/publications.htm

THE QUESTIONABLE "NEED" TO KNOW AN INDIVIDUAL'S ABSOLUTE IDENTITY

7. Many of the concerns uncovered by Trustguide can be addressed by breaking (or, better, never forming) the link between data that describes an individual's characteristics (or his/her actions) and data that defines that individual's absolute identity, eg, full name plus date and place of birth, or National Insurance number. For many types of digital service, the service consumer's absolute identity is not needed, and only a means of paying for the service is required. Such services can be thought of as being similar to real-world services that are paid for in cash and around which the purchaser retains anonymity, eg, a bus journey, a haircut, an entry to a cinema. For some other digital services, eg, online personal healthcare, a link between an individual's characteristics and his/her absolute identity has to exist, in order to ensure that the service is consumed by the intended person. However, even in such situations that link does not always have to be direct; as long as the service consumer can provide proof of some sort that he/she is the intended recipient of the personalised service and has the resources and mechanism to pay for it, then all the needs of both him/her and the service provider are met—the consumer's absolute identity is just not needed for this.

8. Adoption, by public and private sector entities, of digital service delivery systems whose designs minimize (or, better, avoid) the need to know the absolute identity of the service consumer and also minimize (or, better, avoid) the need for information about the service consumer, from which his/her absolute identity can be (easily) derived, would:

- reduce the opportunities for surveillance activity to identify observed individuals absolutely;
- limit those opportunities to situations where there already exists a valid need for absolute identity to be used for service-delivery reasons;
- ameliorate the concerns of individuals about their actions or personal information being linked to their absolute identity, for purposes they have not specifically agreed to, as a result of surveillance activities;
- reduce the risks of theft, loss and abuse of absolute identity information and the consequent costs to individuals and society of the associated frauds;
- ameliorate the concerns of individuals that their online actions increase the risk of falling victim to such fraud or even just receiving unwanted communications;
- reduce the costs borne by service providers to keep large volumes of absolute identity information safe from unnecessary access, secure against loss or corruption due to process/equipment failures and up-to-date;
- enable the observation of online activity *en masse* and the mining of data in large databases to continue to be done, by service providers and others, in order to provide useful aggregated information without the risk of infringing individuals' privacy;

and so increase the perceived safety of, and hence confidence in participation in, the digital economy by individuals, thus helping the Government's vision to be attained.

9. We do not advocate the total replacement of identity-based digital service delivery systems by those in which no identity information at all is required; to do so would allow individuals the freedom to break laws and contracts without risk of being traced and held to account. Rather, we wish to inform the committee of the benefits to be gained if identity information demanded by a service provider, whether public or private sector, be just that required to deliver the service, and no more, thus mirroring the requirements found in the real world. Except where there is a real need otherwise, service delivery systems could be designed to allow consumers to indicate their (partial) identities by means of a set of pseudonyms, ie, tags which are not readily linkable to an absolute identity.

10. We also wish to inform the committee that, following that principle, in many situations digital credentials that assert the right of an individual to consume a service, or assert his/her competence or capability to perform an action (eg, make payment), could be used in place of absolute identity. To repeat a point already made, for many purposes a digital service provider does not need to know the absolute identity of the service consumer—it is merely a convenient way of discovering, labelling, linking and/or tracking the various characteristics of the consumer, which in the process also permits surveillance and exposes the consumer to a range of risks.

11. Some credential-based systems that control access to services, both in the digital and real worlds, require the existence and participation of third parties that are trusted by both the service provider and the service consumer. Typically, such trusted third parties (TTPs) know the absolute identity of a service consumer, and can therefore provide a means for the link between a pseudonym or credential and its owner (ie, the service consumer) to be followed in the event that his/her absolute identity is required, eg, for law enforcement purposes.

12. These abilities of a TTP both to revoke credentials and to reveal absolute identity imply that the digital service consumer must place a high degree of trust in the TTP. However, that is no more than the high level of trust that a digital service consumer today must place in most of the service providers with whom he/she interacts; this is especially true in the case of online financial service providers and most government agencies.

Relevant Digital Technologies for Trust and Privacy

13. There is a variety of technical approaches to providing the individual with the means to manage his/her digital identity information to and control its release and subsequent use. These range from approaches in which all communication and interaction between digital service provider and consumer is done on the basis of anonymous credentials (ie, no identity information is transferred) to those in which the service provider's identity management systems are designed to follow all the consumer's requirements regarding his/her identity information (and thus act as his/her proxy) and are verified as actually doing so.

14. Some of these technical approaches are being further researched and developed within the PRIME project,[166] a 4-year co-operation between 20 industrial and academic research institutions, that aims to advance the state of the art of privacy-enhancing technologies. It is part-funded by the European Union, and its scope includes technologies and system architectures, reference prototypes and application trials, all within a context provided by legal, social, economic and human factors requirements for these. Hewlett-Packard Laboratories is one of the leaders of the project. Within it we have undertaken research and development of technologies that:

- aid a service provider to manage the identity information, provided by a service consumer, according to the requirements of that consumer;
- aid the service consumer to assess the trustworthiness of the service provider's systems, ie, that they will actually manage his/her identity and other information in accordance with his/her wishes;
- aid the service consumer to manage the trust aspects of the device he/she uses to access the digital service;

and work continues on these.

15. Note that two of the above-listed items refer to the trustworthiness of a device or a system. This term is used in a technical sense, and can be defined as the degree of reliance that a device or system will behave as specified, ie, that it has not been corrupted or subverted. Given the present level of cybercrime and likely continuation or steepening of its rate of increase, there is a growing need for both service providers and individual service consumers to have trusted mechanisms for ensuring that their systems and devices are protected against attack and to provide assurance that they have not been subverted (and warnings if they have).

16. Hewlett-Packard Laboratories has been conducting world-leading research into such mechanisms for many years, the results of which have led to open, industry standard specifications[167] for the necessary system components and their use, and to the commercial availability of these components (eg, PCs, laptops, etc.) from a number of vendors. This research and development work continues.

17. Rigorously provable assertions that devices and systems are "trustworthy" are, however, only as valuable as the trust that is placed in the entity making the assertion by the individual or organisation that is considering whether or not to rely on such assertions.

Closing the Loop of Trust

18. The Trustguide project also found that there exists a high degree of distrust of ICT-mediated applications and services ("mediated" means: delivered using a range of technologies), that citizens want more responsibility to be taken by government, the banks and ISPs (Internet Service Providers) and for guarantees to be provided. This implies that citizens would be willing to trust these entities, and in turn this opens up the possibility for them to take on the roles of TTPs for individuals, and also to be part of the chain of trust that supports technical verifiers of software and systems.

19. The existence of such a trust infrastructure would enable the design of digital service delivery systems that rely much less on needing to know the absolute identities of their consumers.

20. To bring this into being would probably require initial support from government. Some reassurance that a critical mass of demand for use of such a trust infrastructure would be generated within a reasonably short timescale would probably be a necessary part of adequately reducing the business risk to investment to create the infrastructure. This may perhaps be less of an issue for financial service enterprises.

21. The Government's ability to satisfactorily provide that support, by itself being a pathfinder provider and operator of a trust infrastructure, is currently questionable, because of the points raised in paragraph 4. However, by making clear statements in support of reducing the use of absolute identities in digital services and by providing open commercial incentives to encourage private sector pathfinders, the Government would be widely seen to be acting to reduce the risks and incidences of exposure to unacceptable digital surveillance (refer to paragraph 3).

[166] PRIME website: http://www.prime-project.eu

[167] These have been developed by, and are available via, the Trusted Computing Group, whose website is http://www.trustedcomputinggroup.org

22. The Government could further enhance its trust rating by supporting the wider use of clear, precise statements of the purposes for which a digital service requests any piece of personal information, thereby helping such best practice become the norm.

23. Such an enhanced trust rating would increase and widen popular support for other IT-intensive government initiatives that are aimed at fighting crime and terrorism and at providing joined-up government services.

Conclusion

24. Hewlett-Packard Laboratories believes that privacy-enhancing and trusted computing technologies have a strong role to play in addressing the privacy issues raised by the increased potential for surveillance over digital service consumers, and that clear statements and actions by Government to support the use of these and other technologies to reduce the use of absolute identities in digital service infrastructures will assist in removing the concerns of (existing and potential) digital service consumers over surveillance and cybercrime, and hence help attain the Government's vision of creating a country at ease in the digital world.

April 2007

APPENDIX 22

Memorandum submitted by Genewatch UK

Executive 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 practice of taking DNA on arrest for a very wide range of offences, and retaining both DNA samples and the computerised DNA profiles permanently is disproportionate to the need to tackle crime.

2. 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 privacy. Issues of cost and cost-effectiveness are also raised by the practice of keeping DNA profiles and samples permanently from so many people. 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.

3. 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 DNA data with other countries will exacerbate this situation.

4. 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.

Introduction

5. 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.

6. Our submission is concerned with the use of DNA for identification purposes and oversight of the National DNA Database (NDNAD). 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. GeneWatch UK strongly believes that there has been insufficient public and democratic scrutiny of these far-reaching and rapid changes. We therefore welcome the opportunity to input to this inquiry.

What is Special About DNA?

7. 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", which can be used to attempt to establish where they have been.

8. 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.

The Role of DNA Databases in Solving Crimes

9. The National DNA Database (NDNAD) relies on the fact that DNA can be taken from any sample of human tissue left at a crime scene. DNA profiles (a string of numbers based on part of the sequence of the DNA) can be obtained from both crime scene DNA and from individuals' DNA (usually collected at a police station using a simple mouth swab) and stored on computer. Every night a 'speculative search' of the Database is run to look for new DNA profile matches. A match between an individual's DNA profile and a crime scene DNA profile indicates a high probability that the individual was at the crime scene.

10. 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: a DNA profile can be obtained from each individual and compared directly with a crime scene profile. For the same reason, a database of individual DNA profiles is also unnecessary to exonerate an innocent person. The "added value" of putting individuals on a database is only to introduce new suspects into an investigation.

11. 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.

12. 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. This is arguably likely to be of most benefit when an individual has a record as a "career criminal" and is considered likely to re-offend.

Expansion and Uses of the National DNA Database

13. Britain's National DNA Database is the largest in the world. It includes DNA profiles from more than 4 million individuals—over 6% of the population, compared to about 0.5% in the USA. The law in England and Wales now allows the police to take DNA samples routinely without consent from anyone arrested in connection with any recordable offence: including being drunk and disorderly, begging or taking part in an illegal demonstration. 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 NDNAD, even if a person is never charged or is acquitted.[1, 2]

14. 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. 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 for all but the most serious offenders.

15. Although the law in Northern Ireland also allows permanent retention of DNA samples and profiles,[4] Forensic Science Northern Ireland (FSNI) still implements a policy of removing profiles on acquittal.[5] However, a recent agreement allowing export of individuals' DNA profiles from Northern Ireland to the NDNAD[6] could lead to changes.

16. The Scottish Parliament voted against permanent retention of DNA from innocent people, in May 2006.[7, 8] Instead, police powers were expanded to allow temporary retention (for up to 5 years) from a much smaller number of people who had been charged but acquitted of a serious violent or sexual offence.[9]

17. A current Home Office consultation proposes further extending police powers (outside Scotland) by allowing DNA to be taken on arrest in the street or in short-term holding facilities (STHFs), in shops or town centres, where people could be detained for up to four hours.[10] Suspected offences for which DNA can be taken would be expanded to include non-recordable offences (such as dropping litter), from anyone aged ten or above. Both computerised DNA profiles and DNA samples would be permanently retained. The main purpose of taking DNA and fingerprints would change from investigating offences to establishing "identity": this implies a new link between the NDNAD and the proposed National Identity Register. STHFs may be staffed by non-police personnel.

18. Uses of the NDNAD may include any purpose related to the prevention or detection of crime. Uses now 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).[6, 11] Undertaking genetic research using the Database or samples is a breach of the usual ethical requirements for consent to such research.

19. Proposals under the Prüm Treaty may in future allow access to the NDNAD, or some of the information it contains, by law enforcement agencies in other European Union countries.[12]

Potential for Abuses and Loss of Public Trust in Policing

20. The NDNAD is a useful tool in criminal investigations, but the permanent retention on it of everyone who has been arrested 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;
- the exacerbation of discrimination in the criminal justice system.

Whose records are on the National DNA Database?

21. More than a million people on the National DNA Database have not been convicted or cautioned for any crime,[13] although some of these people will be awaiting trial.

22. Tens of thousands of children who have never been charged or cautioned with any offence are on the NDNAD[14, 15] The total number of innocent children with records on the Database (including those who had their charges dropped or were acquitted) is unavailable.

23. More than a third of black men in the UK population are on the NDNAD, prompting the Black Police Association to call for an investigation.[16] About three out of four black men between the ages of 15 and 34 have records on the Database.[17, 18]

24. Volunteers, including victims of crime, must give their consent for their DNA profiles to be entered on the Database. However, in England and Wales this consent is irrevocable and cannot be withdrawn.

Potential for abuses

25. 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).

26. When the NDNAD was established in 1995, records were supposed to be removed at the same time as an individual's criminal record.[19] However, 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.[20] The retention of permanent records of arrest is unprecedented in British history.

27. PNC records are available to a wide range of agencies, although a plan is being developed to "step down" records so that access will be limited to the police after similar time-frames to those which used to result in their removal. However, information contained in these records may continue to be made available to others as the result of an Enhanced Criminal Record Check.[21] 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").

28. The permanent retention of these records means there is significant potential for individuals to suffer erosions of their rights simply as a result of a record of arrest. Potential abuses could include: refusal of visas or access to visa waiver schemes (such as that operated by the US); refusal of employment; and excessive Government or police surveillance (of individuals or selected groups of people). The link between the PNC and the DNA Database increases the potential for abuse because an individual's DNA profile can be 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.

29. 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. Although access to the DNA Database itself is supposedly restricted, there have 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.[22]
- 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.[23, 24]

30. The new Home Office proposals for Short-term Holding Facilities significantly increase the risk of infiltration of the system, especially if they give staff who are not police officers powers to check identity using fingerprints and DNA. The risk 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.[25, 26]

Potential for errors

31. DNA evidence is not foolproof: false matches can occur by chance, especially if the DNA profile from the crime scene is not complete. 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[27].

Effectiveness and costs

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. However, such cases do not justify keeping 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.[28] Since April 2003, about 1.5 million extra people have been added to the Database, but the chances of detecting a crime using DNA has remained roughly constant, at about 0.36%.[29]

34. The cost-effectiveness of expanding the NDNAD has never been established.[30, 31] Costs of processing each sample have been made available[32] but do not include police time[33] or the costs of storing samples permanently[34]—a growing part of police budgets.

Unnecessary Retention of DNA Samples

35. Individuals' samples are destroyed in some other countries, such as Germany, once the DNA profiles used for identification purposes have been obtained. Retention of individuals' DNA samples increases privacy concerns and costs (the companies which store them are paid an annual fee). The Home Office has recognised that retaining samples is "*one of the most sensitive issues to the wider public*"[35] and the Human Genetics Commission has concluded that the reasons given for retaining them are "*not compelling*".[36, 37] 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.

The Need for Better Oversight

36. The Government has admitted there is a "regulatory gap" in standard setting for forensic science[38] and GeneWatch UK believes an independent regulator is needed.[39] However, a regulator alone will not address concerns unless a system of time limits on retention, with regulatory oversight, is also implemented.

References

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. The Criminal Justice And Police Act 2001 Chapter 16 amends the Police and Criminal Evidence (NI) Order 1989 so that restrictions on the use and destruction of fingerprints and samples are consistent with the new provisions for England and Wales: http://www.opsi.gov.uk/acts/en2001/01en16-d.htm

5. http://www.fsni.gov.uk/operattxt.html#dna

6. FSNI-PSNI Service Level Agreement 2006–07.

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

8. 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

9. http://www.scotland.gov.uk/News/Releases/2007/01/29133555.

10. Home Office (2007) Modernising Police Powers. Review of the Police and Criminal Evidence Act (PACE) 1984. Consultation Paper. Home Office, March 2007.

11. GeneWatch UK(2006) Using the police National DNA Database—under adequate control? GeneWatch Briefing. June 2006. Available on: www.genewatch.org

12. 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=GAUE2T1MP0CL5QFIQMGCFGGAVCBQUIV0?xml=/news/2007/02/16/ndna16.xml

13. House of Commons *Hansard*. 11 December 2006 : Column 829W.

14. Press Association (2006) MP in bid to wipe DNA profiles. *The Scotsman*. 24 January 2006. http://news.scotsman.com/scotland.cfm?id=116232006.

15. Woolf M, Goodchild S (2006) Surveillance society: the DNA files. *The Independent*, 7 May 2006.

16. Randerson J (2006) DNA of 37% of black men held by police. *The Guardian*. 5 January 2006. http://society.guardian.co.uk/crimeandpunishment/story/0,8150,1678170,00.html.

17. Leapman B (2006) Three in four young black men on the DNA database. The *Sunday Telegraph*. 5 November 2006. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/05/nrace05.xml

18. Rt Hon Baroness Scotland of Asthal, Minutes of Evidence, Home Affairs Committee: Young black people and the criminal justice system. Tuesday 13 March 2007.

19. Home Office Circular 16/95.

20. 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

21. ACPO (2006) Retention guidelines for nominal records on the Police National Computer. 16 March 2006.

22. 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

23. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/AnswerFOI8May.pdf

24. 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

25. Adams L (2006) Police computer goes on the beat. *The Herald*, 14 October 2006. http://www.theherald.co.uk/news/72189.html

26. For example: http://www.itweek.co.uk/vnunet/news/2170113/portable-dna-analyzer-invented.

27. Morgan J (2006) Guilty by a handshake? *The Herald*, 2 May 2006.

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

29. 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

30. House of Commons Science and Technology Committee (2005). Forensic science on trial. Seventh Report of Session 2005–05. HC 96-I, www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf.

31. Williams R, Johnson P, Martin P (2004). Genetic information and crime investigation. August 2004. The Wellcome Trust. www.dur.ac.uk/p.j.johnson/Williams_Johnson_Martin_NDNAD_report_2004.pdf

32. Home Office (2006) DNA Expansion Programme 2000–05: Reporting achievement. Forensic Science and Pathology Unit.

33. HMIC(2000) Under the microscope. p16. http://inspectorates.homeoffice.gov.uk/hmic/inspect_reports1/thematic-inspections/utm001.pdf

34. House of Commons *Hansard*. 8 January 2007 : Column 149W.

35. 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

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

37. 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

38. http://www.homeoffice.gov.uk/documents/cons-2006-forensic-regulator/

39. GeneWatch UK (2006) Standard setting and quality regulation in forensic science: Submission to the Home Office consultation. October 2006. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/HO_consul2.doc

April 2007

APPENDIX 23

Memorandum submitted by Mr Mark Dziecielewski

Given the vast range of activities which your inquiry "A Surveillance Society?" will only have time to skim over, here are a few general points which I would like you to consider:

1. CCTV Surveillance Camera Media Sound Bites

Do not rely on the media sound bites about "4.2 million cameras" or "20% of the world's cameras" or "monitored 300 times a day". These figures are usually quoted without attribution or context. They are only guesstimates by the noted criminologist Professor Clive Norris, http://ccr.group.shef.ac.uk/people/cnorris.htm made over 4 years ago in 2003, so they are probably an UNDERESTIMATE. See: "Estimating the extent, sophistication and legality of CCTV in London", by Michael McCahill and Clive Norris, published in CCTV edited by Martin Gill, Perptuity Press 2003 (now distributed by Palgrave Paladin) ISBN: 189928771X.

2. Automatic Number Plate Recognition (ANPR)

The idea of "roadside" ANPR whereby Police patrols actually stop illegal drivers and their vehicles is welcome. With 30 million vehicles on the road this is a logical policy.

However, the idea of Yet Another National Centralised Database, the National Automatic Numberplate Recognition Database, is very different, especially since the otherwise private vehicle movement data of millions of innocent motorists, who are not being investigated as part of a specific criminal investigation, is being stored for two to six years or more, regardless.

The fact that this database is also to be fed from non-Police operated ANPR cameras, from Local Authorities, Local Police/Community Safety Partnership quangos, and from commercial Road Pricing or Congestion Charging sub-contractors, Supermarkets and Petrol Retailers is a huge privacy and surveillance worry.

There is a history of low paid employees working long hours unsupervised by senior managers eg at night, being involved in Credit Card "skimming" fraud, even with the latest Chip and PIN machines. They have been exploited by international organised criminals and terrorism financiers.

Why should such powerful surveillance technologies, linked to the Police National Computer and the DVLA name and address records of vehicle keepers, be allowed to be accessed by anyone other than real police constables?

3. Data Retention of CCTV Data

The Home Office is involved in European Union wide plans for the mandatory Data Retention of electronic Communications Traffic Data, on 450 million innocent European Union Citizens. This is a stupid, wasteful and privacy invasive policy.

Why are there no corresponding plans to demand mandatory Data Retention of CCTV surveillance camera data for a minimum period eg for two months?

Surely that would make more sense in the fight against terrorism and serious crimes?

4. CCTV Camera Registration

Such CCTV data retention should ideally also lead to the Registration or Licensing of CCTV cameras, which must be beneficial in the critical time period immediately after a serious crime or terrorist incident, when so much police time is wasted hunting down whether CCTV images are available, or trying to find the contact details of the operators.

5. CCTV Warning Signs

You do not need planning permission to put up CCTV surveillance cameras, provided that they do not breach the Building Regulations (no mare than 16 cameras on the exterior of a building, more than 2.5 metres above the ground, smaller than the size of a microwave oven ie all modern cameras now on sale etc)?

However you do need planning permission to put up warning signs that there are CCTV cameras in operation.

The effect of this is that there are more cameras than signs, which is a stupid way to run systems which are meant to deter crime, and lead to gimmicks like "shouting" CCTV systems.

6. National Databases need Single Points of Contact to Investigate Complaints and Errors

The current system whereby each Chief Constable is deemed to be the Data Controller for his regional Police Force, even for data uploaded by his subordinates to a National Database e.g. the Police National Computer, the National DNA Database, the National ANPR database etc. is now unacceptable.

There should be a single point of contact with the actual managers of these National Surveillance Databases,—for the majority of people, it is a bureaucratic nightmare trying to determine even who to contact to complain, let alone get errors corrected.

7. Rectifying Mistakes and Financial Compensation and Apologies

It is inevitable that with the current surveillance technologies, mistakes will be made.

Surely, if we want to make use of these technologies to just and peaceful society, far, far more attention and financial resources should be made available to the rapid rectification of errors, with unstinting and if necessary public, apologies from senior people, and generous financial compensation?

A humane attitude to correcting mistakes, without having to jump through bureaucratic hoops or to have to go to the complexity and expense of a court case, would go a long way in converting the public's suspicion of faceless bureaucratic snooping and surveillance, into an acceptance of these tools as a necessary evil.

I hope that your inquiry will have time to look into some or all of these points.

April 2007

APPENDIX 24

Memorandum submitted by the Finance & Leasing Association

Introduction

1. FLA is the principal representative of the asset, consumer and motor finance sectors in the UK. FLA members achieved £93 billion of new business in 2006. Of this, £65.5 billion was provided to the consumer sector, and FLA members represented 28.8% of all unsecured lending in the UK. The remaining £27.5 billion was provided to the business sector and UK public services. Our members comprise banks, subsidiaries of banks and building societies, the finance arms of leading retailers and manufacturing companies, and a range of independent firms. The facilities they provide include secured and unsecured personal loans, credit cards and store card facilities, leasing, and hire purchase.

2. FLA is heavily engaged in many aspects of the fight against fraud and money-laundering, and of data-sharing. This is not the appropriate place to detail them at length, though we would like to mention here our active involvement in the Home Office's Identity Fraud Steering Committee and several of its working groups. For many years, we have led the calls for greater sharing of relevant data to aid responsible lending and help prevent over-indebtedness. Discussions continue with trade associations represented on the Steering Committee on Reciprocity (SCOR), on the future governance of data sharing with a view to greater transparency.

3. The crucial message we would like to leave with the Home Affairs Committee is that our members, like other lenders, rely heavily on certain aspects of "surveillance". They equally accept that checks and balances are needed and that finding out more about people for its own sake, or for a highly marginal benefit, is not acceptable by society. However, any reversal of the trend towards data sharing would have serious implications for responsible lending, over-indebtedness and financial crime.

Background

4. Some time ago, Richard Thomas, the Information Commissioner, expressed concern that the UK was sleep-walking into a surveillance society. More recently, he has said he is worried that we are in fact sprinting towards a surveillance society. FLA's interest in "surveillance", which for us essentially means data sharing, stems from the need to prevent over-indebtedness and to prevent, detect and investigate financial crime. But, although we are strong advocates of data sharing for these purposes, we do also fully understand the requirement for robust controls to ensure that access to data is restricted to those who have a legitimate need for the data.

5. Consumer behaviour has changed significantly since the days when a consumer would have the majority of his financial arrangements with one organisation for life. 30 years ago, consumers approached their bank manager in person to open an account and saved with a building society for two years before applying for a mortgage. Credit cards had only just been launched. Now, there are 70 million credit cards in circulation. 60% of adults in Great Britain use the internet regularly, and almost half of adult internet users use it for personal banking and financial services. Indeed many people rarely, if ever, go into their bank branch. Now, consumers can apply for and open accounts over the telephone or internet or at a third party such as a store. "Know your customer" has changed from a way of life to a legislative requirement.

Developments in Technology and Data Sharing

6. Consumers as a whole willingly accept and use new technology, notably the internet. It brings them the benefits of greater choice, faster delivery, increased competition and therefore lower prices, constant availability, and a degree of anonymity that many people welcome. But for every plus there is a minus, and criminals deliberately seek to exploit any weaknesses. For FLA members, the biggest minus is the difficulty of knowing their customer. How can lenders be sure that the applicant for finance is who he says he is and can afford to, and will, repay the loan?

7. The Home Affairs Committee will recall that, in oral evidence we gave to your Inquiry in February 2004, FLA continues to support identity cards from a fraud prevention perspective. This is in the absence of a reliable universal form of identity or address verification database in the UK rather than the patchwork of information about individuals that exists across a variety of databases.

8. In a paper on the financial challenge to crime and terrorism, published jointly by the Home Office, HM Treasury, SOCA and the Foreign & Commonwealth Office in February 2007, the Government said that organised criminals used the financial system to move money, and launder and disguise it in other types of assets. In the same way that the financial system provides a mechanism for legitimate trade and investment, so it can be abused by organised criminals and terrorists for their own purposes. The financial sector in the UK relies on its international reputation for integrity and fair-dealing but is itself a target for organised crime, including fraud.

9. However, as criminals and terrorists rely on the financial system, so that financial system itself and the information within it now provide a new opportunity to tackle these threats. Financial information is one of the most powerful investigative and intelligence tools available, the true potential of which is only now being fully understood. Its value is often not fully realised until it is combined with other information. At the same time, criminals capitalise on a lack of routine data sharing. Contradictory information can still be submitted to a range of different agencies without it being picked up. Data-sharing within the public sector is often patchy, while sharing across the public—private divide is rarely even attempted. Happily, the benefits of data-sharing are increasingly being realised across government. For example, pilot exercises in the identity fraud arena and within SOCA are throwing up striking examples of what can be done when public and private data is shared, with particular potential to reduce financial crime, money laundering and fraud. A successful pilot exercise of public sector agencies submitting data to CIFAS, a private sector fraud information sharing service, suggested that a high proportion of address data (on average 31% but as high as 40% for some agencies) matched addresses already identified as being suspect by the CIFAS database.

10. There is significant scope to reduce harm through such mechanisms in a way that strikes the right balance with the need to protect confidential data, as enshrined in the Data Protection Act. Where the Government has information that can help direct private sector efforts to deter money laundering and terrorist finance, it should be shared. This principle is as relevant at the tactical level—for example, sharing details of stolen passports with banks to assess which accounts have been opened with these—as it is at the strategic level—for example, by providing information on the money laundering risks that a firm might exposed to when conducting business in a particular country. The Serious Crime Bill contains important enabling provisions to facilitate more sharing of public sector data.

How Decisions are Made

11. As lenders and customers have become more distant from each other, systems and procedures for assessing risk have had to change. Like anyone else, lenders can only make their decisions based on the information available to them at the time. In risk decisions, that information comes from two or, sometimes, three main sources:

— The consumers themselves, on the application forms.

— Lenders' own records and experience, if the consumers have had a previous relationship with them.

— Credit reference and fraud prevention agencies.

12. Information provided by consumers, however, is of variable quality and accuracy. Many individuals genuinely do not remember the detail sought by lenders and guess or generalise their answers. Those who believe themselves to be a high credit risk omit information or selectively inform a lender of their situation in an effort to ensure that the credit they seek will be agreed. Many people overstate their income when seeking credit. Those who represent the greatest risk have the greatest incentive to withhold information that could be considered negative. And fraudsters lie.

13. Existing or previous customer records are an important and reliable source of information on the behaviour and track record of consumers in managing their credit. However, government policy is to advise consumers to shop around for the best product and deal. This means that consumers are increasingly seeking to transact with new suppliers and are far less likely to approach only their existing lender for a new credit facility. This results in a high reliance on credit reference and fraud prevention agency data for risk assessment.

14. Data is provided to credit reference and fraud prevention agencies by lenders, and then in turn by the agencies to lenders, in accordance with strict guidelines to ensure consistency and accuracy. The use of consistent and accurate credit reference agency data in credit scoring models has led to a significant increase in lenders' ability to assess risk, and this in turn has led to better lending.

Who Benefits from Data Sharing?

15. There are two main reasons why data sharing benefits both lenders and consumers:

— Lenders make more accurate credit decisions more quickly, and are better able to protect themselves against fraud, with increased shared predictive data. This means reduced credit losses, reduced account handling time, and increased lending.

— Shared data means that there is more likely to be early warning of problems for those who may be in financial difficulty, and both consumers and lenders benefit. When lenders become aware that consumers are experiencing difficulties, new applications from those in difficulty are declined, preventing additional overindebtedness. In addition, existing lenders will know to take action to help their customers in the early stages of indebtedness when this help is most effective and when there is a greater chance of a less painful resolution.

— Fuller and prompter sharing of data would greatly reduce the damage which identity theft can cause. The credit industry, including the credit reference agencies, is working on ways of supporting victims of identity theft.

Safeguards

16. The Data Protection Act is a sound piece of legislation that protects consumers' fundamental human right to respect for their private and family life, their home and their correspondence. The response that is needed to the development of a surveillance society is not a change in the law. What is needed is widespread and effective training in the reasons for, and impact of, the legislation, combined with risk-based and effective enforcement. We support the Information Commissioner's work to identify and prosecute "blaggers", and we agree that a custodial sentence can be an appropriate sanction for those who wilfully flout the law. We do not support headline-grabbing, punitive fines against legitimate businesses that take their responsibilities seriously but occasionally make mistakes.

Conclusion

17. Developments in technology have changed the way that businesses and consumers interact. There are undoubtedly benefits for both sides, but downsides, too, and "surveillance"—which for us means data sharing—is an inevitable method of dealing with the downsides. There are risks involved in data sharing, risks of data being abused by criminals, terrorists and others with malevolent intent, but legitimate businesses, the public sector and law enforcement must have access to the same sort of technological tools that criminals use. To help protect consumers' rights, there must be widespread and effective training in the importance of the Data Protection Act, and effective risk-based enforcement of it.

We would once again welcome the opportunity to give evidence to the Committee.

April 2007

APPENDIX 25

Memorandum submitted 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

www.liberty-human-rights.org.uk/resources/policy-papers/index.shtml

Introduction

1. 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*[168] was published. Liberty agrees with the assessment made by the Information Commissioner. 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. We are pleased that the Home Affairs Committee is calling for evidence at this time. However, a word limit of 2,500 precludes any detailed examination of an extremely complex subject. 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.

2. It is useful to clarify what types of activity might be considered "surveillance". "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). 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 purpose unrelated to investigation such as assisting access to public services. 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. Finally, the retention of DNA retained on the National DNA Database (NDNAD) is arguably surveillance. 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. We will make brief observations on all these forms of surveillance along with appropriate conclusions and recommendations.

Mass Informational Surveillance

3. Proliferation of CCTV might attract more observation and comment. However, 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

[168] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

programmes such as the compulsory NIR or the children's index. 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".

4. 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 bill 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.[169] 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.

5. While Liberty does not believe that there is any justification for the NIR, we do not take a similar position in relation to others mass informational databases. For example, we accept that the children's index was created to protect children. We did 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. Information sharing powers were available and Victoria's death was more a result of a catalogue of mistakes and 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 also 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; 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 Primae 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

6. The proliferation of CCTV in the UK is well documented. Hardly a week passes without new newspaper reports of CCTV technology advances. Whether these new generation systems will prove to be of greater use in combating crime remains unproven. Many improvements seem little more than gimmicks. 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 approach to combating crime.

7. Liberty has two principal areas of concern over the use of CCTV. Firstly, it remains effectively unregulated. The legislation that can[170] 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 location for cameras, details on 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[171] but these are effectively voluntary and unenforceable.

7. 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[172] in 2004 has resulted in many systems not being subject to the DPA. The basic position is that CCTV is only covered by the DPA if it can be shown that a system is

[169] As it was the Bichard Inquiry into the killings made the commendable suggestion that a positive vetting process be introduced.

[170] But which often does not. See paragraph 7.

[171] 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.

[172] Durant v Financial Services Authority [2004] FSR28, CA.

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.

8. In March 2007 the Council of Europe Venice Commission published an opinion on video surveillance in public places and the protection of Human Rights.[173] 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.*[174]

Intrusive Surveillance

8. The use of intrusive surveillance is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). This 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. 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.[175] A total of 2,243 intercept warrants were issued in the same 15 month period.[176] 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 originating from overseas need authorisation from a special Foreign Intelligence Surveillance Court. After the September 11 bombings, attempts by President Bush to introduce a limited scheme of executive authorisation of warrants (ie similar to the UK's) was deemed unconstitutional by the US Federal Court.

The National DNA Database (NDNAD)

9. 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.[177] 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 for 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. 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"[178]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

[173] http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

[174] *Ibid* paragraphs 79–81.

[175] "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

[176] "Intercept warrants" allow interception of communications so that the contents of communications can be recorded.

[177] 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

[178] "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.

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 of DNA from those who have not been convicted has helped crime detection.[179] 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

10. As mentioned in the introduction, data mining and data matching techniques are increasingly being used for crime detention. The Serious Crime Bill before Parliament formalises data matching practices in relation to fraud. A recent Home Office White Paper[180] gave details of plans to increase the use of data mining techniques. These practices are a consequence of increased technological sophistication coupled with vast quantities of data held on mass informational databases, making traditional human lead intelligence policing more difficult. 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.[181] 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 from multiple purposes, just so long as the ICO is notified. Notification is essentially an 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.

11. 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

12. 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 the legislative and regulatory framework has failed to keep place with surveillance. The HRA offers recourse to individual action which is of limited use in combating mass data processing. 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 resourcing 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. The role of Parliament needs to be enhanced by ensuring individual Commissioners[182] report to parliament rather than to ministers. As details of information access and sharing are typically reserved for secondary legislation, Parliament should be more readily given the power to amend regulation.[183] Privacy impact statements should be introduced to

[179] 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.

[180] New Powers Against Organised and Financial Crime.

[181] Directive 95/46/EC.

[182] The Interception of Communication Commissioner, The Surveillance Commissioner and the National Identity Scheme Commissioner.

[183] As has happened in the ID card act in relation to the Information that can be recorded I the NIR.

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. Meanwhile, 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.

April 2007

APPENDIX 26

Memorandum submitted by the Home Office

EXECUTIVE SUMMARY

1. Public protection is core to the work of the Home Office and its related services. In order to discharge that duty, we need to be able to respond to 21st Century demands to enable the better prevention and detection of crime, enhance border security, detect immigration abuses and to meet new challenges such as the emergence of new forms of criminal activity and increased threats, whether it is terrorism, identity fraud or internet crime.

2. At the same time technological developments have given us new tools which will help us rise to these challenges. Proper use of these will help build public confidence and security. But 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. It is that balance between privacy and protection that we seek to achieve in all our activities. Public confidence clearly also depends on getting that difficult balance right.

3. This Memorandum sets out the key areas falling to the Home Office, including in particular, CCTV, ID cards and secure passports, the National DNA database, and information sharing. A key theme running through these areas is measures taken to ensure proper and proportionate use, security and safeguards against abuse.

CLOSED CIRCUIT TELEVISION (CCTV)

4. Police experience and research studies show that CCTV has considerable crime detection potential, when used as part of a wider strategy. It can also reduce fear of crime. Its use has attracted accusations of invasion of privacy.

5. The first legal control of CCTV in public areas was the Data Protection Act 1998. The definitions in the Act are broader than those of the Data Protection Act 1984 and more readily cover images. The legally enforceable standards previously applied to those processing personal data on computer now cover CCTV and are based on the eight Data Protection Principles.[184].

6. The Information Commissioner will take into account the extent to which the users have complied with the CCTV Code of Practice when determining whether they have met their legal obligations. The code deals with surveillance in areas to which the public have largely free and unrestricted access.

7. 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.

8. The report of the review will be published shortly.

AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

9. ANPR has proved to be a very successful operational tool allowing the police to intercept a wide range of criminals using the roads.[185]

10. There are a number of Government departments and other organisations[186] that operate ANPR systems. We aim to enable, through statutory powers, the bulk sharing of information between such operators and specified law enforcement agencies, to facilitate the prevention and investigation of all levels of criminal offending (but particularly terrorism and serious crime) while ensuring that effective safeguards are in place.

[184] Data must be: fairly and lawfully processed; processed for limited purposes and not in any manner incompatible with those purposes; adequate, relevant and not excessive; accurate; not kept for longer than is necessary; processed in accordance with individuals' rights; secure; not transferred to countries without adequate protection.

[185] The arrest rate is between nine and ten times higher than that of general patrol officers, increasing the number of offences brought to justice by three times the national average.

[186] for example the Highways Agency and Transport for London.

The National Identity Scheme

11. The *Strategic Action Plan for the National Identity Scheme*[187] set out the Government's plans to provide more secure and reliable ways of proving identity, including more secure passports and the introduction of Identity cards (ID cards). The Scheme is not designed as a surveillance tool. It will protect individuals' identities from abuse and provide a secure way for people to prove their identity more reliably, helping to tackle illegal immigration, crime and terrorism as well as improving public services.

12. The Identity Cards Act 2006 establishes a National Identity Register which will hold the identity information, including biometric information, of everyone issued with an ID card. The Border and Immigration Agency (BIA) will start to issue biometric immigration documents to foreign nationals in 2008 and the Identity and Passport Service will begin to issue ID cards to British citizens from 2009.

13. *Checking National Identity Register information:* When a person applies for an ID card any information to be recorded in the National Identity Register will be checked against a number of public or private sector data sources[188] to help verify the person's identity.

14. *Verifying identity with consent*: The Scheme will also allow a more secure and reliable method for individuals to prove their identity to private sector organisations, (such as banks) by providing their ID card and, with the person's consent, for this to be verified against the National Identity Register. However the user organisation will not obtain access to the National Identity Register.

15. *Provision of information without consent:* The Identity Cards Act 2006 will also enable the provision of information from the Register without an individual's consent but only in strictly limited circumstances such as for the prevention and detection of crime.

16. *Safeguards:* There are a number of safeguards to ensure that the National Identity Register information is held securely:

- Separate IT systems will hold National Identity Register biographical and biometric information and will be accredited by the government's security authorities.
- A National Identity Scheme Commissioner will be appointed to oversee the operation of the Scheme. The Intelligence Services Commissioner and Tribunal have a specific remit to deal with how the intelligence services use any information provided from the Register.
- There will be rigorous auditing, staff access restrictions, alerts and a range of technical controls to guard against internal misuse.
- Any unauthorised disclosure of information from the Register will be a criminal offence.[189]

National DNA database

17. The National DNA Database (NDNAD) is a publicly owned police intelligence database,[190] It is governed by a Strategy Board chaired by ACPO with membership from the Home Office and the Association of Police Authorities. The Custodian of the NDNAD is accountable to the Board ensuring, amongst other things, that all profiles added to the NDNAD are reliable and compatible. The standards and procedures for the supplier laboratories are set by the Custodian.

18. Section 64 of the Police and Criminal Evidence Act (PACE) provides that fingerprints, DNA profiles and samples taken in connection with the investigation of an offence may *only* be used for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution, or the identification of a deceased person or of the person from whom a body part came.

19. Companies which analyse DNA samples and produce profiles for the NDNAD have to be accredited under the International Quality Standard for Testing Laboratories, ISO 17025. The companies store DNA samples and profiles on completion of analysis in case they need to be re-examined in the future and are required to do so in a secure environment.

20. *Existing safeguards for data use:* Safeguards are provided by the restrictions imposed by PACE and the Data Protection Act, 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.

21. *Profiling:* The DNA profile of an individual consists of a code number which represents the person's gender and ten markers from areas of DNA which do not play an active role in determining personal characteristics. The NDNAD therefore is not and will not be used in any attempt to correlate particular genetic characteristics with propensity to commit crime. However the NDNAD does allow different unsolved crimes to be linked to the same offender or offenders, which is one of its important benefits.

[187] Published in December 2006.

[188] These provisions will be established in secondary legislation under Section 9 of the Identity Cards Act 2006.

[189] With a maximum penalty of two years imprisonment while tampering with the Register will be subject to a maximum penalty of 10 years imprisonment.

[190] The database is operated by the National Policing Improvement Agency which is a Home Office-sponsored Non-Departmental Public Body which vested in April 2007.

Facial Mapping

22. A national facial image database is currently being developed. This will enable police forces to share more efficiently the images they currently hold on individuals with each other for operational investigative purposes.

Electronic Monitoring

23. Electronic Monitoring (EM) has been operating throughout England and Wales since 1999. The monitoring service is provided by two private security firms under contract to the Home Office. They also initiate enforcement action as necessary. Contractor staff are subject to Criminal Record Bureau (CRB) checks.

24. EM is used predominantly to monitor a curfew condition. Adults or juveniles can also be monitored on bail, as a court-ordered community sentence or on release from prison. The technology only monitors a person's presence or otherwise at a specified address, not their general whereabouts.

25. 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 Data Protection Act. The release of such information must be approved by the Home Office unless the subject is a Multi-Agency Public Protection Arrangements (MAPPA) or Prolific or other Priority Offender (POPO) case.

Regulation of the Investigatory Powers Act 2000

26. 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).

27. RIPA is 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 to safeguard national security or to prevent and detect crime.

28. Subject to various statutory safeguards and oversight, this conduct includes:

- interception of communications;
- covert observation and eavesdropping on conversations in private spaces, both premises or vehicles;
- covert observation and eavesdropping on conversations in public spaces and vehicle location tracking;
- covert interference with private property; and
- acquisition and disclosure of communications data.

29. 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. RIPA also provides access for complainants to an independent tribunal—the Investigatory Powers Tribunal.

Criminal Records

30. The Home Office has a policy interest in the recording, retention, disclosure and quality of criminal record information held by the police. In addition to sponsorship of the Criminal Records Bureau and its parent legislation, this includes the arrangements for the disclosure and notification of such information, by the police, outside of the CRB disclosure service.

Data Sharing—General

Data-sharing between government departments and agencies

31. The *Data Protection Act 1998* (DPA) regulates the collection, use and distribution of personal data. The Government is committed to more information sharing between public sector organisations and service providers, and is equally committed to ensuring that once data is shared it will be kept safe and secure.

Existing safeguards for data use and whether they are strong enough

32. Greater data sharing and proper respect for an individual's privacy are compatible. Safeguards are essential to prevent unnecessary or disproportionate intrusions into individuals' privacy. The balance is maintained by the good legislative framework we already have in place which allows data sharing but guarantees individuals' legitimate rights to privacy through the Data Protection and Human Rights Acts.

33. The Government is very keen to tackle the misuse of personal data where it occurs. Following recommendations by the Information Commissioner and a DCA consultation, Government proposes to increase the penalties available to the Courts by amending section 60 of the DPA. This will enable those guilty of offences under section 55 of the DPA to be imprisoned for up to 2 years on indictment and up to 6 months on summary conviction. Government will seek to introduce legislation as soon as parliamentary time allows.

Information Sharing between Police Forces—IMPACT

34. The IMPACT Programme is introducing new IT enabled business change to improve the ability of the Police Service to manage and share its intelligence and other operational information in order to prevent and detect crime. It 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).

35. All forces and agencies sharing information for policing purposes remain under a strict duty to conduct activities in a lawful and appropriate manner and the Programme is addressing the legal and policy issues in close partnership with the Service, the Home Office, DCA and the Information Commissioner. A statutory code of practice on the Management of Police Information (MoPI) was introduced in November 2005.

Multi-Agency Information Sharing

36. The Crime and Disorder Act 1998 provides the power to disclose information lawfully to enable crime and disorder reduction partnerships to tackle crime and disorder. More recently arrangements have been put in place for information sharing to prevent serious violence.

37. *Information sharing to prevent serious violence:*. Multi-Agency Public Protection Arrangements (MAPPA) are the statutory arrangements set up in 2001, under the Criminal Justice & Court Services Act 2000, to provide a mechanism for agencies to work together when they are dealing with offenders who are assessed as posing a high risk of harm to others or whose risk management is exceptionally problematic.

38. The police, probation and prison services constitute the "responsible authority" who must co-operate with other specified agencies, and one form this co-operation will take will be information-sharing.

39. The Home Office is currently rolling out Multi-Agency Risk Assessment Conferences (MARACs) to provide a standardised approach to public protection for victims of domestic violence. The role of the MARAC is to facilitate, monitor and evaluate effective information sharing.[191]

40. The Home Office is looking at ways in which it might introduce processes to improve multi-agency risk assessment, information-sharing, management, and interventions to prevent serious violence in circumstances where MAPPA and MARACs would not apply.

Fraud and the Serious Crime Bill

41. The Serious Crime Bill provides a legislative gateway for public authorities to share information for the purpose of preventing fraud through a designated anti fraud organisation. The Bill also provides a statutory gateway by which public and private sector bodies can contribute their data to the Audit Commission for the purposes of undertaking data matching in order to prevent or detect fraud. It also makes the contribution of data for such purposes mandatory for some bodies, in particular local government and NHS bodies.

42. *Existing safeguards for data use:* Neither provision authorises any disclosure of information which contravenes the Data Protection Act 1998.

43. The Bill provides a specific offence and penalty for wrongful onward disclosure of HMRC information It imposes criminal sanctions in circumstances where an individual discloses information in breach of statutory limitations. The Bill also places a statutory duty on the Audit Commission to produce a Code of Practice in relation to data-matching, and for all those who are participating in data matching exercises to have regard to this Code.

[191] In Cardiff, where a MARAC has been operating, repeat victimisation has reduced from 30% to less than 10% from 2004–06.

IMMIGRATION

44. The Border and Immigration Agency (BIA) deals with a vast number of immigration applications every year, including over one million in-country applications alone. All immigration applications contain personal information which is received, stored and used in a number of ways.

45. *Intelligence:* BIA's Intelligence Directorate works to combat serious & organised immigration crime, enhance border security and detect abuses of the immigration system. This involves data sharing between Government Departments and Agencies, the maintenance of secure intelligence databases and profiling on the basis of intelligence and risk.

46. *E-Borders Programme* delivers a modernised integrated secure border control system across all modes of transport. It is a multi-agency approach to tackling immigration and customs abuse, serious and organised crime and counter-terrorism. Passengers can be identified, assessed and cleared by relevant border agencies before departure to and from the UK, using information gathered by airlines as part of their current processes. Information sharing under the programme will be governed by a code of practice which will be published and laid before Parliament.

47. *Iris Recognition Immigration System:* IRIS (Iris Recognition Immigration System) is delivering a biometrically controlled automated border entry system for pre-registered travellers at 9 airport terminals in the United Kingdom. The system provides a fast, fraud-resistant way to pass through automated barriers at UK immigration controls.

48. *Enforcement:* BIA's enforcement priority is to remove the most harmful people first and the key sanctions for high-harm immigration offenders are removal or deportation. Electronic monitoring is used to maintain contact with individuals both to encourage compliance with the asylum and immigration processes and also enable an increase in the rate of removal. In 2007–08, we intend to increase our use of electronic monitoring, in particular the use of electronic tagging or voice verification.

49. *UK Borders Bill:* The UK Borders Bill provides for information sharing between the Agency and the HMRC and contains a specific criminal offence for the unlawful disclosure of HMRC information to prevent the misuse of sensitive tax data.

April 2007

APPENDIX 27

Memorandum submitted by 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.

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.

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 detrimental unjustified consequences. 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. 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. Breaches of security can have even more significant consequences and there is great potential for more discrimination, social sorting and social exclusion. 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;
- a climate of fear, suspicion or lack of trust.

The Importance of Data Protection

7. The risks of excessive surveillance—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.

8. 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?

9. 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. 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 on which to base 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.

10. The Commissioner does not believe that we 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.

11. 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".

12. 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

13. The Commissioner's 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.

14. 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.

15. 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

16. 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 extent of identifying particulars needed to provide services, thereby reducing the associated data protection risk. The ICO is sponsoring a strategy forum at the Oxford Internet Institute (7 and 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

17. 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 who 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.

18. 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. 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. 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.

19. 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 of the wider public sector to seek the Commissioner's opinion on particular types of developments at a early stage. It is possible that such a requirement could be incorporated into the privacy impact assessment procedure.

Powers

20. 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.

21. 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.

22. 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

23. 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.

24. 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.

April 2007

APPENDIX 28

Memorandum submitted by Mr G M Walkley

Kindly accept this document as written evidence to be placed before the Home Affairs Committee.

My primary concern in relation to the subject of a surveillance society is one of principle. Which is that as a citizen of a democratic country we do not live by permission of the government. A government is elected as the servant of the people, not its master. We have a right to privacy and freedom and only allow our government to curtail these freedoms in very limited and important circumstances. It is not a proper function of government to involve itself in surveillance of law-abiding citizens, or to establish systems of compulsory identification, nor open files on each person.

1. Many individuals have details of themselves recorded on private databases and these should only be available to public agencies in specific circumstances. It should be obligatory on the agency attempting to access a private database to place the a request for such access before the judiciary who will decide the validity of the action.

2. This is a matter of trust. If a government believes that the general population is untrustworthy then they will do their utmost to prove any misdemeanour by insisting that data is shared by all departments and agencies. To suggest that measures such as ID cards will combat terrorism or wipe out benefit fraud is to capitulate to those who perpetrate the crime. One has to bear in mind that the criminal element in our society is in the minority and that the law abiding majority should not be criminalised. Therefore I submit that it is not necessary to take DNA from those not convicted of a criminal offence, nor to fingerprint our schoolchildren, or to have a national identity register. These are but a few of the measures that are being introduced to monitor the masses.

3. The safeguards suggested by the Government will never be enough as no computer system can be regarded as secure-one only has to look at the recent extradition of a UK citizen to the USA for hacking into the Pentagon computer systems to see that this is true.

4. Abuses will inevitably take place as the scope of these systems and those that can access them are vast. It is for this very reason that the Minister of State for Children, Rt Hon. Beverley Hughes, when referring to questions raised said that "records of children whose circumstances may mean that they are at increased risk of harm may be the subject of shielding". She goes on to say that unauthorised access will be prevented by using a combination (unspecified) of measures. As already stated in item 3 no computer system is secure.

5. We have just recently received confirmation that criminal elements have been targeting credit/debit cards used at petrol station in the UK. A sophisticated scam has taken place not very long after the introduction of the Chip and Pin. How long will it be before the criminal fraternity hack into the National Identity Register when it is up and running?

6. All these databases that have been or are being introduced by the Government impact on the privacy of the individual citizen and impinge on our human rights. We the electorate cannot allow this to continue.

In conclusion I would say that this is a very serious breakdown of trust! We elect our Members of Parliament on the basis of trust and expect them to reciprocate that trust. Without trust between our elected representatives and the individuals who voted for them the very basis of democracy is threaten. It is recognised that CCTV cannot now be rolled back however I would strongly urge Parliament to consider the consequences on introducing more draconian measures and indeed reversing some that have been allowed to become law.

April 2007

APPENDIX 29

Memorandum submitted by the Identity Trust

INTRODUCTION

1. Identity Trust is a proposed initiative to create a Community Interest Company[192] (CIC) initiative focused on building tools and processes that enable transparency and more equitable user/ supplier relationships. Identity Trust is member of the ITU-T Focus group on Identity Management, a member of the Internet Governance Forum: Dynamic Coalition on Privacy at the UN, and the US based Identity Commons. Currently identity Trust is being consulted by the OECD focus group on Identity Management for input into guidelines to facilitate the development of regulatory standards for national identity management.

2. Identity Trust is in the process of raising investment funding to facilitate and extend the development of commercial guidelines for the emerging Identity Industry. This emerging industry is being compared to the Telecommunications Industry crossed with the Credit checking industry and will prove to be a commercial example to which the government surveillance practices will be measured by.

3. it is the intention of this submission to advise on the role of transparency and the use of transparency in a reciprocal manner to the use of surveillance over people and their identity data. The more surveillance and the greater the scale and use of that transparency of people and their identifiers, the greater the need transparency, and user visibility needed over the management, manipulation, purpose, and sharing of that data. Eg User Identity Management logging, with read, write, aggregate, and

4. For instance a citizen needs to see who has accessed, for what reason, what their data is being data mined for—etc. This would be consistent with commercial and international developments in international Identity Management standards.

5. The United Kingdom is in significant danger of becoming a laggard country in terms of its approach to privacy, data protection and "identity" due to issues of trust. This will become an economic issue as well as a privacy one in that individuals will have options to take at least some of their "business" to other countries with more robust and user centric Identity Management approaches in place.

"Legitimate governance is inextricably linked to the larger problem of trust on the Internet. Market forces alone have proven insufficient to build trusted public networks. Trust is essentially a political problem rather than a technology or legal issue. For greater trust, the millions of individual participants in the Internet must find some vehicle for co-operation. Their own ability to trust will depend on the choices made by others on the network. A 'trusted' network goes beyond engineering concepts and requires a system that allowed users to feel confident that data and messages were confidential, unmodified and linked to an identity. Progress in building secure and trusted public networks requires asking what are the policies and legal and regulatory structure needed for trust; how would these be coordinated among nations; and who is best placed to undertake these actions." Jamie Lewis, Perils and Prospects for Internet Self-Regulation, Center for Strategic and International Studies, June 2002.

6. Surveillance and inappropriate identity management can erode trust and undermine the overall UK governance infrastructure .

7. Risks of this could include the dispersion of commerce (Banking, Legal, Intellectual Property, etc.) to other countries where more favourable conditions exist.

8. This contribution to this inquiry is intended to highlight solutions to the systemic issues surveillance creates in society. Surveillance and IdM practices that occur today that minimise user/customer/citizen transparency and thus create lack of trust and ultimately commercial disadvantage can in turn stimulate an open marketplace and drive commercial innovation in the UK.

BACKGROUND

9. The quote below from the National Consumer Council in 2004[193] neatly summarizes the dilemma being addressed in this consultation exercise.

(a) 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.

(b) 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

[192] http://en.wikipedia.org/wiki/Community_interest_company
[193] The Glass Consumer, 2004.

> 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.
>
> *Source:* National Consumer Council, 2004.

10. That's the theory; 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:

(a) The rapid increase in the use of surveillance and tracking technologies with little in the way of "opt out" possibilities.

(b) An ever-growing mountain of irrelevant junk mail on their doormats, and other forms of direct marketing messaging grabbing their precious time.

(c) Cold-call tele-marketers blatantly using hard sell "slamming" tactics to sell products and services that are not in the individuals' best interests.

(d) 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 paymsters that selling personal data is within their remit).

(e) 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.

(f) The increased risk identity theft, with all that this entails, from organizations taking less care of personal data than they should.

11. In order to map a positive way forward for all parties, as suggested in the above quote, we must articulate the strategic weaknesses in the current state, and then put new modus operandi in place that are un-encumbered by these outdated mind-sets and processes.

Specific Current State Problems

12. Specific problems with the current state include.

13. The Data Protection Act, and the various add-ons of recent years are articulated at too high a level to be meaningful. The various acts fail to enable meaningful transparency around:

(a) Precisely what data are being stored (split by sensitive and non-sensitive data).

(b) Precisely how long are they being stored for, and how is there accuracy maintained.

(c) Precisely what are these data being used for.

14. The answers to all of the above are largely available to organisations, through processes typically relating to data audits for major IT projects (e.g. CRM, business intelligence, analytics). An example of such as audit is shown belo.[194] But, the Data Protection Act does not demand disclosure at this detailed level, allowing organisations to hide behind obscure, high level descriptions enshrined in privacy policies that are specifically designed not to be read by end users.

15. This current scenario is best summed up by quoting from a top UK-based data protection lawyer about how they engage/support their business colleagues—'the business people tell us what they wish to do, and we tell them how to do it to avoid getting caught out by data protection law'. This start point is wrong—the personal right to privacy is not a priority for organisations, whether they be private or public sector.

16. Most organisations have in-built structural reasons for not wishing to be transparent about data content stored, and data uses deployed. In the private sector the motive is profit (driven by shareholders), in the public sector it is reducing "cost to serve". (driven by stakeholders) If customers or citizens actually knew, through transparent approaches, what was being done with their personal data, then they would minimise sharing and usage using existing legal vehicles and further steps available (eg the various suppression files). Until this barrier is overcome, then we won't move beyond the current mess.

17. There is no mandatory requirement for notification of a data breach (USA used to be regarded by Europe as having weak privacy laws, yet in Califiornia they are streets ahead in how they handle the inevitable data breaches).

18. Data Protection legislation has not kept pace with the developing internet and e-commerce world. Web 1.0 is stretching enough, but the far more personal data-intensive web 2.0[195] will be the straw that breaks the camel's backs of the current approaches.

19. In light of web 2.0 and what will come next (see below), the right to subject access must be modernised in a number of respects.

---

[194] This data audit process (one of many available), breaks data content down into 75 data types, data quality into 10 components (eg completeness, compliance), and the use of data into 90 types (eg customer lifetime value analysis for marketing, data mining for fraud management).

[195] A good summary can be found in the book *The Digital Person* http://docs.law.gwu.edu/facweb/dsolove/Solove-Digital-Person.htm

20. Success rates for crime detection via CCTV are low in practice due to the inadequacies of the current state technology.

21. Current approaches show no respect for the time of the individual. Time is increasingly a more scarce commodity than money and should be treated as such.

SUGGESTIONS

22. Update the Data Protection Act (an equivalents) to articulate data content and data usage at a meaningful level of detail.

23. Introduce Privacy Impact Assessments as an overlay for new projects—but based on this new, lower level of detail. At the high level, PIA's would be meaningless (and thus an un-necessary layer of bureaucracy).

24. Mandatory, value-added data breach notification . . . a "no-brainer"—don't debate, just deploy.

25. Further research and educate on the principles of minimal disclosure (ie only gather and store the data required rather than take the opportunity to grab more).

26. Investigate revenue sharing with individuals whose data is being sold (start with DVLA).

27. Investigate the impact on the time of the individual wasted by data related weakness.

28. Publishing of success rates by CCTV camera and having each installation justified would minimise un-necessary deployment.

29. Improvements to the subject access process should include:

(a) The data subject should be provided with the data relating to them in electronic format should they wish.

(b) Cost of subject access should fall to expand usage (which in turn will aid the whole eco-system).

(c) Frequency of subject access should be targeted at "any time, and almost real time".

(d) Automated use of agents (electronic and manual) to aid individuals in subject access requests should be encouraged.

30. Fund research into the use of digital rights management around personal data—one of the few ways in which privacy legislation can actually be enforced. Pilot such schemes in government databases to track/make transparent data sharing and data use.

31. Accept that without much of the above, individuals will gain transparency anyway through the much more aggressive deployment of Privacy Enhancing Technologies (PET's).

April 2007

APPENDIX 30

Memorandum submitted by the Human Genetics Commission

I would like to begin by saying that Members of the Human Genetics Commission (HGC) are grateful for the opportunity to contribute to this Home Affairs Committee Inquiry. As Chair of the HGC's Identity Testing Monitoring Group, I have been asked to submit a response on behalf of my fellow Commissioners.

The HGC is the Government's advisory body on new developments in human genetics and how they impact on individual lives, with a particular focus on the social, ethical and legal issues. The Commission is chaired by Baroness Helena Kennedy QC and is made up of twenty-three members including experts in genetics, ethics, law and consumer affairs. We also have a Consultative Panel of people who have direct experience of living with genetic disorders and who act as a sounding board for our reports and recommendations.

It is clear from the press notice relating to the Inquiry that it will examine broad issues relating to modern security and surveillance techniques and their wide implications for British citizens. The Commission has an interest in the storage of human genetic information and has monitored the use of genetic databases for research, medical and forensic purposes since its inception in 1999. Our interest within the context of this Inquiry is two-fold. Firstly, we have concerns about safeguards relating to research and genetic databases. Our understanding of genes and of how they work in the human body is the result of prolonged and extensive research efforts. If this understanding is to be translated into therapeutic benefit, such research must be given every encouragement. Sustained public confidence and participation is therefore vital.

Secondly, in terms of the forensic use of genetic information, the HGC has been closely involved in overseeing the operation and management of the National DNA Database. In May 2002, the Commission published its report *Inside Information—Balancing interests in the use of personal genetic data,* which contained several recommendations calling for robust ethical oversight of the work of the National DNA Database custodian and the Database profile suppliers. Further, it recommended that the Home Office and

Forensic Science Service introduce an independent research ethics committee, to approve such research proposals which involved the use of database samples—a recommendation which is currently being implemented by the Home Office.

Following publication of *Inside Information*, the National DNA Database Strategy Board invited the HGC to put one member forward to sit on the Board and this arrangement has continued to this day. I myself took over as HGC representative on the Board, when I joined the HGC in 2001. In late 2006, following continued lobbying by the HGC for additional ethical oversight of the database, the Chair of the National DNA Database Strategy Board wrote to Baroness Kennedy QC, to ask that a second member join me on the Board. This arrangement—two HGC Members sitting as lay-members on the Board—was formalised, so that it will continue even if the HGC ceases to exist or its remit changes in the future.

Due to the time and drafting constraints attached to this submission, it will not be possible to fully explore the issues as we see them in any detail. For this reason, I enclose a copy of the *Inside Information* report together with the Executive Summary for your interest.[196] The Commission has discussed and commented on the use of personal genetic information many times but, in my view, this report addresses the key issues and areas of concern in a clear and comprehensive way. In particular, I would like to draw the Committee's attention to Chapters 5 and 9, which look at medical research and personal genetic information and forensic uses of genetic information.

Our overriding concern in respect of the growth of private and public genetic databases is the risk that they pose to research and to medical care if they are accessed for purposes that fall outside the original remit for which the information has been collected. One of our key roles is to promote debate and listen to the public on matters relating to human genetics. Earlier this month, the Commission held a public meeting in Edinburgh with the ESRC Genomics Policy and Research Forum to discuss the Scottish genetics research database, *Generation Scotland.* It was evident from audience questions and comments that there was real anxiety around the possibility—however unlikely—that the police might gain access to genetic collections such as UK Biobank and Generation Scotland. We all have an interest in successful genetics-based medical or health-related research and our concern is that public anxiety in this area could affect people's willingness to collaborate with the NHS or in research to the long-term detriment of us all.

As a Commission, we recognise the National DNA Database as a powerful criminal intelligence tool. However, there is a danger that its value in terms of crime detection and reduction could be used to justify the erosion of important freedoms, without prior analysis of the risks and benefits as to the likely good that may accrue from breaching privacy in the short term against the loss to society in the long term, as a result of citizens withdrawing their cooperation.

It might interest you to learn that the Commission, in partnership with the ESRC Genomics Forum, and PEALS and with the support of the Sciencewise programme and the Wellcome Trust, intends to commission a Citizens' Inquiry on the forensic use of genetic information. This deliberative event will involve a small, inclusive group of UK citizens who will be able to call witnesses, review, assess and discuss evidence and address key questions and concerns about the forensic use of DNA, specifically the National DNA Database. The group will consider social, legal, ethical, economic and scientific factors and will be able to express their views on a number of key questions, some of which will be posed to the group and others defined by the citizens themselves. Findings and recommendations made by the group will be published and submitted to Ministers. The Commission also intends to respond to the on-going Government consultation, to look at the potential to review the Police and Criminal Evidence Act.

We would be happy to provide you with further information concerning the HGC should you need it and would very much appreciate being kept up to date on the progress of your work in this area.

April 2007

APPENDIX 31

Memorandum submitted by the Action on Rights for Children

1. During the past five years, developments in IT 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.

2. Manufacturers of commercially-available devices have exploited the marketing opportunities presented by popular concerns such as child abduction, obesity and bullying, while the government's "risk management" approach to children's policy has emphasised the use of IT solutions to monitor and share information about children in an attempt to detect early signs of problems. In-depth assessment and profiling tools have been developed that are believed to predict potential criminality, social exclusion or educational failure on the basis of statistical probability.

[196] Not printed.

3. Taken together, these developments have significantly eroded children's privacy rights, guaranteed by Article 8 of the European Convention on Human Rights and reiterated by Article 16 of the UN Convention on the Rights of the Child. It is now possible for a child to be under near-constant scrutiny throughout each day.

4. Because the expansion in the use of IT has been piecemeal, there has been no overview of the possible combined effect on children's development of the various technologies. There is certainly the potential for children to become conditioned to accept a far higher level of surveillance than society now tolerates. Given that privacy and decisions about self-disclosure are a powerful means of regulating our relationships with others, consideration needs also to be given to the effects of surveillance on a child's maturing sense of personal boundaries and autonomy.

5. It should also be borne in mind that over-confidence in technological solutions and poor standards of information security can threaten the integrity of children's personal information, and may even place children at increased risk of harm from hacking and careless or corrupt disclosure of data by those with legitimate access.

Government Databases and Assessment Tools

6. The wide range of children's databases and assessment processes is extensively covered in the FIPR report to the Information Commissioner: *Children's Databases—Safety and Privacy* available online at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrenspersonal_information.pdf

7. Given the limitations of space, the complexity of the entire database system and the large number of data protection, human rights and consent issues that it raises, we cannot possibly do justice to the subject matter here. We believe that it would be more helpful to the Committee for our briefing to concentrate on the other areas that affect children's privacy. However, the Director of ARCH is a co-author of the above report and it therefore provides an accurate reflection of our views and concerns. We respectfully suggest that Committee members consider it essential reading.

Commercially Available Surveillance Devices

CCTV and Webcams

8. There is increasing use of CCTV in schools, and monitors may even be placed in pupils' toilets. Images can be relayed via Internet Protocols to control centres located outside school, where they are accessible to local council staff.[197]

9. There is also a growing trend towards using webcams in nurseries to enable parents to view their children via a password-protected internet system. As the webcam monitors an entire room, all parents can see all of the children at any time.[198] Some systems allow parents to nominate others, for example grandparents and family friends, who may view the webcam. Parents cannot therefore know who else is watching their child.

10. Children are not asked to consent to the use of CCTV. In the case of nursery webcams, all of the advertising concentrates on the psychological benefits to parents. No consideration is given to children's dignity and privacy, nor to the fact that, while parents may feel involved in their child's day, this is not a reciprocal relationship.

Biometric systems

11. Electronic systems are increasingly used in school canteens to monitor children's individual school meal choices, and in school libraries, where children's reading habits can be monitored individually, and also by ethnicity and gender. Many of these systems use children's fingerprints, which are converted into an algorithm that is stored on the school system.[199] Some schools are also introducing fingerprint scanners for school registration.[200]

12. There is mounting protest that children's fingerprints are being taken without parental consent, and concerns that templates are transferable between systems.[201] This raises the possibility that the data could be used by other agencies for other purposes. Although manufacturers claim that a child's fingerprint cannot be reconstructed from the algorithm, this is a red herring; all fingerprint systems now use algorithms derived from a fingerprint, rather than the fingerprint itself.

---

[197] See for example: http://www.surveillancenewsportal.com/surveillance_news.asp?articleid=26640&arttitle=Alarm-triggered%20CCTV%20systems%20increase%20security%20at%20Wigan%20school

[198] Example: http://www.thisislondon.co.uk/news/article-23392356-details/Big+Mother+is+watching+you/article.do

[199] Extensive information can be found at: http://www.leavethemkidsalone.com/

[200] http://www.vericool.co.uk/home.html

[201] Kim Cameron, Architect of Identity and Access, Microsoft Connected Systems Division http://www.identityblog.com/?p=743 See also various posts between 27 March–1 April.

13. Because the data is held on school computers in relatively insecure buildings, its security cannot be guaranteed. Burglary and theft from schools is not uncommon, and the growing importance of biometrics is likely to make databases that hold biometric data a target for organised crime. Manufacturers offer assurances that the data is encrypted using 128-bit encryption techniques, but developments in computing will undoubtedly render such assurances meaningless within a short time. Even if a child's data could be considered safe today, it is unlikely to remain so, and the problem is exacerbated if schools do not ensure the complete deletion of data from a computer hard-drive.

14. We have been told that "guidelines" for schools on the use of children's fingerprints will be published on the British Educational Communications and Technology Agency website during May; however, these will not in any way be binding on schools. We remain deeply concerned that children's biometric data may be compromised by theft; that the data may be misused, and that children will become habituated to giving up their biometric data far too readily. In our view, the increasing importance of biometrics for security-critical functions means that they should not be used for low-level purposes.

Location-based services

15. There are a number of companies selling location based services to parents. These purport to enable parents to track children via their mobile phones, by logging on to a website that displays the whereabouts of the phone. Parents can also pre-set boundaries and routes, and receive alerts if their child deviates from them.

16. A new generation of GPS tracking devices and mobile phones is now coming on to the market; we are told that "Mobiles2Go"[202] is about to launch a major marketing programme that will see its 'i-kids' tracking phone placed on sale in supermarkets and High Street stores. We are also aware of a device called the "KinderGuard"[203] currently under development: a location device that also includes biometric sensors to transmit details of a child's heart rate and skin temperature to parents. This indicates when a child is under stress, and also lets parents know if their child has removed the device.

17. There is no statutory regulation of any of the above devices, beyond the Data Protection Act 1998. Providers of mobile location services have agreed a voluntary code of practice,[204] but this does not include any requirement that service providers should undergo police checks. An attempt to amend to the Safeguarding Vulnerable Groups Act 2006 to introduce such a requirement was resisted by government. [205]

18. Although the code says that devices: "*should not be marketed in any way which exploits parents' concern or fear that their child may become a victim of crime*", it is clear that some companies are very close to this line.[206]

DNA Retention

19. On 4 April 2004, police powers were extended to allow DNA profiles, fingerprints and other information to be taken without consent from anyone arrested on suspicion of a 'recordable offence'. The police may keep this information indefinitely, even if the person arrested is never charged, or is subsequently acquitted.

20. With the help of MPs and the Children's Commissioners, we have made repeated but unsuccessful efforts to obtain accurate Home Office figures for the number of children on the National DNA Database (NDNAD) who:

(a) did not receive any disposal or further action;

(b) received a reprimand or final warning.

21. Using the Youth Justice Board figures for juvenile arrests and disposals, we believe it is possible that DNA profiles of around 200,000 children who have received no disposal may be on NDNAD, and a further 200,000 profiles of children who have received reprimands or final warnings.

22. The existence of a child's profile on NDNAD puts the onus on him/her to justify the presence of his/her DNA at a crime scene, and may lead to unwarranted suspicion. Although this is equally true of adults, children are at far greater risk of injustice. Almost one quarter of arrests are of 10-17-year-olds, and the range of databases holding sensitive information about them has considerable potential to prejudice the position of those whose records include predictions of the likelihood of future criminality. We are profoundly concerned that whenever a positive DNA match is made, the police will access other information held on the child, and that this will create a set of assumptions that will influence police attitudes, including the likelihood of guilt.

[202] http://www.mobiles2go.com/m2g/

[203] http://www.kinderguard.co.uk/technology/

[204] Code of Practice for the use of passive location services in the UK: http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf

[205] Commons *Hansard* 23 October 2006 Col 1244: http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm061023/debtext/61023-0005.htm

[206] See eg Childlocate website front page: http://www.childlocate.co.uk/

23. It is extremely important that children and young people are kept out of the youth justice system unless there are no other options left, and recognition of this fact has led to the reprimand and final warning schemes. There is also a growing body of evidence that arrest and/or questioning by the police has negative effects on young people's behaviour. The Edinburgh Study of Youth Transitions and Crime, a ten-year longtitudinal study of 4,000 young people that began in 1998, found that:

> *". . . being caught by the police had a particularly strong influence on whether young people gave up delinquency entirely: the more times they had been caught by the police, the less likely it was that their level of delinquency would be zero at either sweep 5 or sweep 6."*[207]

The explanation offered for this finding is that young people find it very hard to escape from being labelled "criminal". There is a real risk that the presence of a young person's profile on NDNAD will lead to disproportionate police interest and questioning when there is no other evidence of involvement, and lead to increasing anger and alienation on the part of the young person.

24. We are concerned that speculative familial searches are being conducted on NDNAD. This has the potential to cause great difficulty and distress to those children whose paternity is not as they had assumed,[208] those who are adopted, and those who have changed their identity because they are escaping domestic violence or are subject to witness protection.

25. In our view, it is entirely wrong to retain the DNA of children and young people who have not had any action taken against them, or who have been acquitted by a court.

26. Retaining the DNA profiles of those who receive reprimands and final warnings defeats the purpose of the scheme, which is to prevent young people from entering the youth justice system for low-level, often first, offences. It increases the likelihood of further contact with the police and risks "locking in" young people to the criminal justice system, rather than providing them with an opportunity to change their behaviour before they are faced with more serious consequences.

27. Where a child has been convicted of an offence in the courts, we believe that DNA profiles should only be retained in line with the Rehabilitation of Offenders Act 1974.

April 2007

APPENDIX 32

Memorandum submitted by Mrs A Jones

SUMMARY

The main problem in using technology to develop efficient and effective systems lies in "control". Information is a valuable commodity to business and we have seen our data "sold on" to maillists etc without consent. Government wishes to "control" our data and by default our lives. Individuals fear a "loss of control" over the volume of personal information held and the uses to which it may be put.

Commercially we have moved away from the huge, all-encompassing databases of the 1980's because these databases were slow and cumbersome to use, inflexible and had great potential for inconsistency and error in the data they stored, eg: BACs system too slow to pay all salaries on Friday 30 March 2007. The trend is now towards smaller, simpler systems that are cheaper to implement, use and maintain and which can be linked to other databases as and when necessary.

The issue of privacy and data protection remains critical and while all efforts should be made to develop secure systems it is not possible to guarantee any system against hackers or unauthorised access; eg: recent theft over 45 million customer records from TK Maxx and recent news that junior doctors' job applications have been accessible on the internet.

The key to success lies in the design of the system. For example, keep personal identifying data to a minimum—full name; date of birth; full address, mother's maiden name etc—is it essential? Would initials and surname do? Personal identifying data should be kept on a separate database. The administrators working with the system should not see the personal information and the two parts of an individual's records would be linked only by a unique reference code. The computer system could link the two records where necessary eg: to sent out a letter, but joining the two parts of the individual record should be virtually impossible either by a legitimate system user or by an individual with criminal intent. Updates to records in response to, for example, changes in legislation could continue to happen as this would be an "across the board" change to all records meeting certain conditions.

---

[207] Edinburgh Study of Youth Transitions and Crime: "Social Inclusion and Early Desistance from Crime" *David J Smith*: *http://www.law.ed.ac.uk/cls/esytc/findings/digest12.pdf*

[208] BBC News "Who's the Daddy?": http://news.bbc.co.uk/1/hi/uk/3023513.stm

For any access to an individual record, eg due to change in circumstance or response to a query, the record holder would provide their unique code (but no other personal data) and this would also serve to imply the consent of the record holder. To further reduce system size, vunerability and improve efficiency, thought could be given to splitting a database into several small systems based on criteria like "Place of Birth" or "Age band".

All systems should have a "time out" facility built in to prevent unattended data remaining visible on screen.

All systems should have a detailed Access Log recording every access, time, date, user and reason for access.

A record should be made available at any time to the individual record holder of all accesses to their record and of any requests for information from third parties.

A Code of Practice should be drafted to clearly state the responsibilities of systems users and the penalties which will be applied for Misuse of Personal Data stored within a system. There should be a clear and simple procedure for individuals to view and correct their records and to make a complaint if they feel their data has been misused.

An "Opt Out" should be available to everyone for every new system, with the aim that through "best practice" over time when a system is shown to work people may decide to "opt in". This provides a level of individual control and will perhaps encourage people to view new systems with less suspicion. For example, in "private business" individuals have a choice of whether or not to apply for a loan, have a store card or loyalty card etc.

Access by Public Agencies to Private Databases

In what circumstances would this be necessary? If an individual was suspected of involvement in fraud or other criminal activity, the public agency or police should already have some evidence on which to base their suspicions and if the individual under suspicion did not give consent to further investigations then an application for a Warrant from a Court of Law should remain the appropriate procedure. It does not seem appropriate to suggest government agencies should "fish" databases looking for inconsistencies or suspicious activity without good cause.

Aside from criminal activity, what other purposes could exist here? Would, for example, the NHS monitor individual's shopping with a view to banning them from buying junk food or cigarettes? Any purposes for this type of access should be clearly defined and debated. Where such a request for person-identifiable information is made perhaps permission should be sought from the individual, or at the very least the individual should be informed of the action and its purpose.

The obvious danger of this "partnership" is that it would work in two directions. For example, would a mortgage lender or a pension provider be able to access an individual's health record? Would a Curriculum Vita automatically be created on-line from various databases for a potential employer to download?

The likely result of this type of "partnership" is that people will stop using "systems" as far as possible eg: people will reject reward cards, store and credit cards, and will return to using cash.

Data–Sharing Between Government Departments and Agencies

The current system prevents the sharing of data between agencies and this privacy is protected by legislation. Merging or splitting government agencies and departments should not be used as a way to circumvent this system. As now, a Warrant can be applied for where reasonable evidence exists to suggest an illegal activity has taken place.

Better and quicker communications between departments/agencies should be built-in where it is necessary to confirm or clarify—for example—that a person's contributions are sufficient for a claim for a state benefit. This is not "data sharing"—this is a simpler "Yes or No" response to a query.

Existing Safeguards for Data Use and Whether They are Strong Enough

The current legislation that protects privacy and prevents data-sharing is fairly robust, and should be further strengthened in light of the new, current and future systems under discussion. There is a need to be open and to state exactly what data is required and for what purpose it will be used. Any links from one database to another need to be stated and explained. Data should not be used for any other purpose without individual consent.

The Monitoring of Abuses

No one individual or team should be given control of or access to a complete individual record. Personal data could be managed within the system eg: to send out a letter but should not be readily available to any system users. All access should be closely controlled and monitored, eg: only the data essential to a particular task should appear on the screen. A full electronic log should automatically track and record each access. An extremely robust system of penalties for unauthorised access, misuse of data, divulging information to

a third party etc must be clearly set out and made available to system users and to members of the public. Investigations into misuse and the issuing of penalties must be adhered to. This is a "new" crime which should be treated very seriously. It is currently difficult to prove a breach of confidentiality has taken place and this process needs to be simplified and all steps taken to ensure transgressions are investigated and acted upon where necessary.

Potential Abuse of Private Databases by Criminals

The abuse of any database system—public and private—cannot be underestimated. It may prove impossible to protect any system from hackers or from data theft or misuse. Even "chip and pin" is not foolproof. Iris scans, DNA and fingerprints are not feasible for a routine administrative system, and will perhaps not prove to be accurate or cost-effective. The larger the system the greater the risk, and therefore it is essential to consider system design. If someone decides to "acquire" an individual's tax records, for example, these will be of no real use if the personal identifying information is held elsewhere on a separate system. The task of acquiring the two separate parts of the record becomes much harder. The splitting of the record into further parts will again make the "acquisition" harder.

The onus on system security must lie with the system owner, and this could lead to the system owner becoming financially liable to compensate for distress or other effects of data abuse.

The Case for Producing Privacy Impact Assessments

Advertise in the national press for case studies from people whose lives have been affected either by the information stored about them or by the way in which that information has been used. A large number of "ordinary, decent" people have already been adversely affected by this and use of real case studies should be viewed as an essential part of system design, to minimise or remove "unfairness". A current example is the many people who have worked hard and lived decent lives for years but who now find their employment activities are curtailed because of CRB disclosure of "spent" crimes.

Privacy-enhancing Technologies

The issue of privacy does not lie within "technology". It rests with system design, safeguards, system users, and clearly defined guidelines of acceptable use with penalties for any other use. The danger of technology is the speed and ease with which information can be found. A person may have been reluctant to break into a locked store room to look through thousands of paper-based files for personal information, but can now use a PC to access the same information in seconds. The temptation to a low-pay administrator to acquire and sell-on this information must be great therefore the solution is to limit the information an individual administrator can access.

In what way will our privacy be enhanced or protected if we are required to give our full name, date of birth, address etc to estate agents, banks and building societies, shops, solicitors, doctors, hospitals, government agencies, schools, colleges, insurers, pension providers, current and future employees etc. Currently many of these bodies take and keep a photocopy of a Passport or a Driving Licence, making it much easier today to collect sufficient personal information to use in a criminal way than was previously possible. An ID Card containing all our personal data seems something of a gift to someone with criminal intent. Club membership cards and soon bank cards will be totally blank cards which can only be activated by authorised terminals and will then only divulge relevant information about the holder. Even this is unlikely to be "fool proof" for long.

April 2007

APPENDIX 33

Memorandum submitted by Transport for London

1. Introduction

1.1 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.

1.2 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.

2. Use of CCTV

2.1 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.

2.2 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.

3. Working with Other Agencies

3.1 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.

3.2 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.

3.3 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.

3.4 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.

4. Conclusion

4.1 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.

April 2007

APPENDIX 34

Memorandum submitted 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 notion of a "surveillance society", which we understand to mean the use and extent of surveillance (including the gathering of personal data on individuals) by both the public and private sector in modern Britain. Surveillance can sometimes be a

legitimate tool (eg in the fight against crime) and few would dispute the usefulness of such developments as search engines and databases. But such advances also have an obvious potential to interfere with personal privacy if not properly regulated.

3. For this reason, JUSTICE has long been concerned with the impact of various kinds of surveillance[209] and data-gathering activities—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,[210] 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 of the various measures that engage personal privacy. Instead, it deals only with the broader human rights issues arising from surveillance and data-gathering.

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,[211] 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' (i.e. whatever is not prohibited by statute is permitted),[212] privacy was traditionally protected by the *absence* of legislation

[209] 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.

[210] 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).

[211] 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].

[212] 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.[213] 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.[214] 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.[215] 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.[216] 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".[217]

11. 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, e.g. 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-gathering.

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*.

[213] 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].

[214] 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".

[215] 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).

[216] 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 41at 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".

[217] 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".

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.[218] 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.[219]

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.[220]

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.[221] 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.[222] 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".[223]

18. Similarly, in our recent report on intercept evidence,[224] 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[225] and US[226] federal governments on the use of electronic surveillance with the paucity of information available under the report of the UK Interception of Communications Commissioner.[227] 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

[218] 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.

[219] 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.

[220] We use the term CCTV generically. As the Royal Academy of Engineering report notes, n2 above, p 33: "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. The continued use of the term is an indicator of a general lack of awareness of the nature of contemporary surveillance, and disguises the kinds of purposes, dangers and possibilities of current technologies".

[221] *Peck v United Kingdom* (2003) 36 EHRR 41.

[222] Cf 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".

[223] *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

[224] *Intercept Evidence: Lifting the ban* (JUSTICE, October 2006).

[225] See eg Public Safety Canada, *Annual Report on the use of Electronic Surveillance—2005*.

[226] 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*.

[227] See eg *Report of the Interception of Communications Commissioner for 2004* (HC 549; SE/2005/203).

recently held unconstitutional by the US federal courts.[228] 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.[229]

April 2007

APPENDIX 35

Memorandum submitted by the Association of Chief Police Officers

CRIME BUSINESS AREA

SUMMARY

The Association of Chief Police Officers welcomes the decision of the Home Affairs Select Committee to conduct an Inquiry into "the surveillance society". The Inquiry provides an opportunity to reflect on the extent to which an appropriate balance has been struck between the Article 8 Rights of Citizens on the one hand and the need to suppress criminality on the other.

The Select Committee has adopted a very broad definition of surveillance. The definition contained within the relevant legislation is narrower, yet it still manages to be a source of great confusion within the law enforcement community, as do several other concepts on which the legislation relies. Taken together, recent and future technological advances, and the experience of several years of the regulation of Investigatory Powers Act 2000, give good reason to take a fresh look at the current range of definitions used within the legal framework for covert investigation.

Directed and Intrusive surveillance, CCTV, Automated Number Plate Readers (ANPR) and data retrieved from a range of other sources are fundamental to effective law enforcement. Together they have saved many thousands of lives and have prevented thousands of citizens from becoming victims of crime. The benefits are felt across society and help us manage threats ranging from neighbourhood anti-social behaviour to international terrorism.

Since 2004, ACPO has participated with the Home Office in a joint review of the Regulation of Investigatory Powers Act 2000 (RIPA). The review has recommended changes to the primary legislation to remove unnecessary bureaucracy, to redraft the codes of practice and to develop better mechanisms for providing guidance to police and other law enforcement officials. ACPO believes that covert surveillance and intrusive techniques should be properly authorised and accepts that this process will, of necessity, need to be appropriately recorded. But the regime that has developed around RIPA has become unnecessarily bureaucratic and has been characterised by a risk-averse approach that has proved wasteful and has hampered investigations.

ACPO believes that the supervisory and inspection arrangements around the police use of covert techniques are unnecessarily complex and could be simplified. While the use of surveillance techniques by public authorities is highly regulated, the same is not true of their use by private individuals and businesses. In particular, CCTV systems are operated by many businesses where no clear standards have been established and there has been no registration, inspection, training or enforcement. The quality of much equipment (and the subsequent evidential product) is variable. Sophisticated surveillance equipment is readily accessible to private individuals from a range of open sources. The inquiry provides a welcome opportunity to reassess this, although ACPO would not encourage the development of a regulatory regime that would be costly or which would discourage use of private CCTV.

In Summary, ACPO would welcome:

— An acknowledgment of the fundamental value of surveillance, in its broadest sense, to crime investigation and reduction.

— A reduction of unnecessary bureaucracy.

— A rebalancing of control between the highly regulated enforcement sector and other users of surveillance.

[228] See *American Civil Liberties Union v National Security Agency*, US District Court, 18 August 2006 (Case no 06-CV-10204).
[229] See our 1998 Report, Recommendation 2, pp 19–22.

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.

Submission to the Home Affairs Select Committee

ACPO welcomes the Home Affairs Select Committee Inquiry into "a surveillance society". The Inquiry has implications for a broad range of ACPO work portfolios and working groups. This initial submission to the Home Affairs Select Committee is intended to simply highlight several broad areas that ACPO feels might benefit from scrutiny as part of this Inquiry. These are:

- definitions;
- CCTV;
- data retrieval and other techniques;
- the regulation of Investigatory Powers Act 2000;
- the regulatory regime; and
- the non-regulated use of surveillance.

Definitions

The Home Affairs Select Committee has adopted a very broad interpretation of "surveillance"'. It extends beyond the conventional concept of directed surveillance which is defined within RIPA. The Review of RIPA (see below) found that even this limited concept was open to confusion and misinterpretation. The risk of misinterpretation grows as the scope of what we mean by "surveillance" is broadened. Technological advances also broaden the possibilities available to law enforcement agencies and others. Taken together, these considerations suggest that the time is right for a review of these definitions and an improvement in our ability to articulate what we mean by each term.

RIPA has little to say about the scope of surveillance: it would be helpful to articulate a differentiation between "watching" and "seeing", for example. Similarly, there is a distinction between "live surveillance" and the acquisition of "historic" information. A debate would be welcome on when data becomes "historic"—what if it is retrieved from a system that recorded it a matter of seconds ago? Practitioners also struggle with the distinction between visual surveillance and electronic surveillance, and with the concept of "private information"—especially in public places. Technologies exist today that were scarcely envisaged when RIPA was enacted. They provide great opportunities to criminals and the law enforcement community should be equipped with a framework to use them appropriately, too.

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 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 40 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; and

— 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 seventeen 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.

Regulation of Investigatory Powers Act 2000

RIPA was enacted in 2000 to provide the framework which would enable law enforcement bodies to interfere with individual Article 8 Rights when there was good reason to do so. It gradually became a source of more and more complaint to Ministers, Members of Parliament and senior police officers. Officers found the legislation, or at least the way in which it had been interpreted, to be a source of unnecessary bureaucracy.

Responding to these concerns, a review of the legislation was launched in 2004. The Review explored a range of intrusive techniques, including directed surveillance, the acquisition of communications data, intrusive surveillance and covert human intelligence sources.

The Review found that the legislation had several ambiguities and deficiencies, although many of the problems that had been identified were linked to the way it had been implemented. 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 borne of a generally "risk averse" approach. This risk aversion, and continues to mean to this day, that there is little in the way of case law to guide investigators and Senior Investigating Officers—as the prevailing "safety-first" mindset offers little prospect of a challenge in the courtroom.

ACPO continues to work with the Home Office to develop a single source of advice and a reliable doctrine or guidance document for use by investigators.

ACPO urges the Home Affairs Select Committee to consider the case for making amendments to RIPA: amendments which acknowledge the need for appropriate levels of recording, but which would encourage the reduction in the inappropriate bureaucratic burden that has developed since RIPA was enacted.

The Regime for Inspection and Regulation of Police Surveillance

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—HMIC. The Commissioners' officers work entirely independently of each other and adopt different methodologies, have different styles and do not co-ordinate their inspection activities.

Several police forces report bidding farewell to one inspection team a matter of days before welcoming a team from a different inspectorate's office. ACPO believes that bureaucracy could be reduced and greater cohesion and efficiency achieved by exploring the establishment of a single Commissioner for activities governed by RIPA.

Unregulated Surveillance

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 prosecutions 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.

The Home Affairs Select 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 unregulated, users of 'surveillance'. It would be, however, disadvantageous to introduce a regulatory regime that is costly and which discourages the use of private CCTV.

April 2007

APPENDIX 36

Memorandum submitted by the Department of Health

The Committee has announced that the focus of its inquiry will be on Home Office responsibilities, but that it will also look, where relevant, at those of other departments, and has mentioned in that context "databases being developed by the Department of Health". We have interpreted this as a reference to the NHS Care Records Service (NHS CRS).

The following evidence is very largely drawn from written evidence recently submitted to the Health Select Committee in connection with its current inquiry into electronic patient records.

Executive Summary

The NHS CRS will, in due course, provide a nationally available, secure, lifelong patient record that holds patient demographic data and, from 2007, will start to hold summary clinical information such as allergies, adverse medical events, medication etc. Access is via secure smartcard technology, available at the point of need by healthcare professionals who have a role based, legitimate relationship with the patient.

We believe that holding summary care records, and doing so on a national database, will deliver very significant benefits for safety and the efficient management of NHS services, improving healthcare outcomes for millions whilst preventing thousands of unnecessary deaths.

In all cases, access to records will only be permitted to the staff of organisations involved in the care of NHS patients, working as part of a team that is providing a patient with care, and will be limited to only as much information as is needed for the purpose of the care or other job role being performed in relation to the patient. Where those providing care are not NHS staff then patients will be informed of this and any objections raised respected.

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 to restrict access to their clinical information, and clinicians responsible for treating them have a duty of care to explain to those who choose to do so the potential impact their decisions may have on their future care. If nonetheless a patient does not want important data to be available to other than those who have collected it, even though absence of that information may lead to future harm, they will have the right to seal the information and accept the consequences.

It will be open to individuals to choose not to have a summary care record at all.

Patient information that will be held on the new local and national electronic record systems, and the options patients will have to prevent their personal data being placed on systems

Clinical Information

1. The recording of clinical information is a matter for professional regulation and will also depend in part on policies and protocols in local NHS organisations. Doctors are required by the General Medical Council 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. Other health professionals have similar obligations.

Demographic Information

2. Patients' demographic details are already held in the Personal Demographics Service (PDS), a key component of the NHS Care Records Service. It is estimated that in the region of 3.5 million patients per annum change GP Practices and for an increasingly mobile population, and with an ever more diverse range of NHS healthcare providers, the PDS provides a consistent accurate source of demographic information. This includes items such as:

— name;
— address;
— date of birth;
— NHS number; and
— Current GP.

3. Currently, in a typical week, 6.5 million messages are processed by the demographics service which is accessed on a typical NHS day by 50,000 authenticated unique users. The total number of queries to date now exceeds 230 million. As a result of the central personal demographics database some three quarters of a million letters per year are now correctly addressed. The introduction of the Personal Demographic Service (PDS) at University Hospital Birmingham has seen a reduction from 3% of misdirected letters down to 0.44%, improving overall accuracy rates for patient correspondence to 99.56%.

4. Access to the Personal Demographics Service (PDS) will reduce clinical risks arising from a failure to match patients with their clinical record, and help minimise cases of correspondence and documents being misdirected. Currently, some trusts send tens of thousands of misdirected items of mail a year, and nationally the figure runs into millions of items. Early evidence from one trust has shown a six-fold reduction in misdirected mail addressed using data held in the Personal Demographics Service (PDS), with a saving in postal and staff-related costs that would translate into many millions of pounds nationally per year.

5. People registered with the NHS will not be able to prevent their basic demographic and contact details from being held within the NHS CRS. The NHS has maintained registers of its service users from the earliest days of its existence and for a variety of reasons to support the delivery of healthcare.

6. 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.

7. Access to the Personal Demographics Service (PDS) by NHS staff is restricted to those issued with a smartcard and an appropriate role. 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. Further, whilst it is not practicable to give patients choice about whether their demographic details will be held in the system, safeguards have been built into the PDS which allow an individual's contact details to be hidden from NHS staff if they request this level of protection. These safeguards, termed sensitive flagging or shielding of records, were developed originally for witness protection and similar cases but are now available for all patients who have strong concerns about NHS staff accessing their contact details. It is intended that all staff involved in care who need to access demographic information, even those who are not employed directly by the NHS, will be subject to at least the same levels of registration as NHS employees when being granted access to patient information.

Summary Care Record

8. The Summary Care Record forms the national element of the NHS Care Record Service and will provide authorised healthcare professionals with access to key clinical information about a patient anywhere at any time. Piloting of the Summary Care Record, part of the NHS Care Records Service (NHS CRS), in "early adopter sites" will begin from Spring 2007. The ready availability of information about patients in the Summary Care Record will help prevent medication errors which cause 1,200 unnecessary deaths a year in England and Wales. It will also help reduce unnecessary admissions to hospital particularly of older people The Summary Care Record will be created by copying data currently held within GP systems with the agreement of the GP Practices concerned. At first, the Summary Care Record will contain only basic information such as known allergies, known adverse reactions to medications and other substances (eg peanuts) acute prescriptions in the past six months and repeat prescriptions that are not more than six months beyond their review date.

9. In due course more information will be added about current health conditions and treatment. "Adverse drug reactions (ADRs) continue to represent a considerable burden on the NHS, accounting for 1 in 16 hospital admissions and 4% of the hospital bed capacity. Most ADRs were predictable from the known pharmacology of the drugs and many represented known interactions and are therefore likely to be preventable. Over 2% of patients admitted with an adverse drug reaction died, suggesting that adverse effects may be responsible for the death of 0.15% of all patients admitted" (Source : BMJ abstract of research at two general hospitals in Merseyside—BMJ 2004; 329:15–19).

10. Discussions are under way with representatives of the medical professions, patients and the public about the final scope and implementation of the Summary Care Record. Experience in the early adopter sites will be thoroughly evaluated before wider roll-out of the Summary Care Record.

11. Individuals who have concerns can choose not to have a Summary Care Record created for them. They will be advised to inform their GP of their views and to request that a note be made of their concerns and the choice they have made. The GP practice may ask the patient to sign a form indicating that they understand and accept that it may not be possible for the NHS to provide them with the same care as others receive in circumstances where the Summary Care Record will enable improved care. They can alternatively choose to have a Summary Care created but not accessible to anyone but themselves. They will be able to access it anytime using a secure internet site called HealthSpace. Patients will of course be able to change their mind and request a Summary Care Record at any point.

Detailed Care Record

12. Records containing information about a patient's medical care exist currently in a variety of places, for example, at their GP surgery or at hospitals where they have received treatment but at present they cannot easily be shared. Over the next few years, as the NHS Care Records Service (NHS CRS) develops, NHS organisations such as hospitals, clinics and GPs will be able to share their electronic records where appropriate. This may vary from area to area depending on the physical infrastructure. A patient who has attended NHS organisations in different areas may have more than one set of shared detailed records.

13. The detailed care record component of the NHS Care Records Service (NHS CRS) will support the care process and will typically contain:

- Name;
- address;
- date of birth and NHS Number;
- past and current health conditions, allergies;
- assessment, investigations and diagnosis including test result and digital images;
- care plans and reminders;

— treatments including operations and medications; and

— care reviews and discharge information.

14. Individuals may ask those who are providing care for them whether or not it is possible to withhold information from the new IT systems but in many cases this will be impracticable. Some forms of care, X-rays, laboratory tests etc will generate records within the new systems automatically and the only way to prevent this is to choose not to have that particular care or treatment. Where clinicians feel that they can keep adequate records outside of the new systems there will need to be robust arrangements for clinical audit in order to assure the quality of care and protect patient safety. The Department of Health is to conduct a consultation on processes for managing patient requests of this sort. However, even where information has to be held within the new systems, patients have considerable control over who may access that information as described below. Alternatively, people can choose to have their information held electronically but not accessible to anyone outside the organisation that created it—thereby recreating an electronic version of the *status quo*.

How third-party access to locally and nationally held clinical and demographic information will be managed and controlled

15. Only the duly authorised staff of organisations that are involved in providing care will have access to confidential medical information held within the NHS Care Records Service (NHS CRS). Such staff will need to have a "legitimate relationship" to access the information in an individual patient's record and will only have access to system functions, and hence to data, as required by their role. Organisations that are not involved in providing or supporting the delivery of health and social care, will not have direct access to any confidential medical data.

16. 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, but public interest rules for disclosure to the police or other agencies are not changed by the introduction of the NHS Care Records Service (NHS CRS). In rare circumstances, the law or the Courts require clinical information to be disclosed and requirements such as these must necessarily be met. This is exactly the same as what happens now with paper records and non-linked computer systems.

17. Demographic data—contact details—has not always been held under the same strict rules of confidentiality as clinical data but some individuals provide their contact details in circumstances where confidentiality needs to apply. To reflect this, and also to reflect the importance that the Department of health places on sustaining the trust of patients, as a matter of policy all patient demographic data is treated as if it were confidential for most purposes. Such data is therefore only disclosed to support health and social care or under the same public interest rules as clinical data or where there is a statutory basis for the disclosure.

Protecting Patient Confidentiality

18. The benefits of the NHS Care Records System (NHS CRS) for both patients and NHS staff depend on safeguarding sensitive patient information from inappropriate disclosure. The NHS Care Record System provides a set of technical access controls and audit facilities that, along with the professional standards of staff in the NHS, safeguard sensitive patient information from inappropriate disclosure. They provide much more rigorous controls than exist now for either paper records or existing electronically held records.

19. The Department of Health sets stringent standards for patient confidentiality and has taken the lead in government in developing a comprehensive privacy statement in the form of the NHS Care Record Guarantee, articulating in plain language precisely what NHS organisations must do to meet legal and policy requirements. The Department is also strongly supporting the Information Commissioner in seeking stronger penalties for breaches.

20. 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 National Programme are contractually bound to auditing their adherence to these.

21. The NHS Care Records Service (NHS CRS) incorporates stringent security controls and safeguards to prevent unauthorised access to personal information and to detect potential abuse. These 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 and is providing the NHS with a set of security tools to deliver centrally determined standards.

22. The Department is aware that some patients will not be reassured by NHS security controls and is therefore providing patients with choice about participation in many of the new developments. 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.

Security Controls Managed by the NHS

23. Users (healthcare professionals) 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 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" governed by NHS Connecting for Health. 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. Where suspect behaviour is identified, local trusts will follow their procedures for investigating staff.

24. 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.

25. 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.

26. 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.

27. NHS organisations must undertake to observe strict conditions to ensure the NHS CRS is used appropriately, and users are required to sign up to a set of conditions for use of the smartcard. These obligations and conditions are complemented by the various existing codes of conduct and professional responsibilities by which all NHS staff are bound. Actions which do not conform to them, which includes the sharing of smartcards, are dealt with locally. Sharing of information between members of a team has happened routinely prior to the introduction of smartcards, but we recognise that the sharing of smartcards could undermine the assurance that patient confidentiality will always be appropriately respected. Staff who breach patient confidentiality are subject to professional disciplinary measures. Offending doctors and nurses will be reported to their professional regulatory bodies and may face additional disciplinary action, including losing their licence to practice.

Options and Controls available to Patients

28. Patients have a number of options. They were developed following extensive research and consultation with patients/carers/citizens and the NHS.

(i) Not to have a Summary Care Record (SCR) by requesting this through the GP Practice where they are registered. Individuals who opt-out of having a SCR may change their minds at any point in the future. Electronic prescriptions and electronic bookings are also optional.

(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.

(iii) To have their address and contact numbers hidden so that they are not available to NHS staff. Whilst the NHS is legally required to hold non-clinical patient contact details for all patients where these can be obtained, this option has been provided so that even the most concerned individuals can still receive care and have joined-up records.

In time, patients will also be able to have an SCR but to designate some data items as sensitive so that they cannot be viewed outside of the team that recorded the information without the individual's express permission. This type of control is referred to as a "sealed envelope".

Disclosure Overrides: Court Orders, and the Public Interest Test

29. Whilst all information held by a doctor about a patient is subject to the requirements of the Data Protection Act 1998, and patients' consent to share, and ability to limit the sharing of their care record, is covered by the NHS Care Record Guarantee, circumstances may arise requiring authorised users of the care records database to open sealed envelopes without patients' permission. In part this will depend upon the type of information that patients choose to seal. For example, the law requires some forms of communicable disease to be notified to the National Patient Safety Agency, so if a patient sealed information about this, the information would be extracted without the patient's permission.

30. Where information is sealed it will be opened without specific permission only where there is an explicit statutory requirement to disclose information, as in the above example, where a Court orders the disclosure, or where the holder of the information determines that the public interest outweighs the patient's right to confidentiality, for example in cases of serious crime or where there are significant risks to other people. By their nature, these will be very unusual circumstances.

Use of data held on the new systems for purposes other than the delivery of care eg clinical research

31. 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 introduction of the NHS Care Records Service (NHS CRS) represents a major opportunity for supporting the secondary analysis and reporting of information for a variety of purposes. 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).

32. 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.

33. 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.

34. 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.

35. 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.

36. In January 2006, the new national health research strategy *Best Research for Best Health* announced that the Department of Health would ensure the capability exists within the national NHS IT system to facilitate, strictly within the bounds of patient confidentiality, the recruitment of patients to clinical trials and the gathering of data to support work on the health of the population and the effectiveness of health interventions. The UK Clinical Research Collaboration established an expert group under Professor Ian Diamond, Chief Executive of the Economic & Social Research Council, to advise NHS Connecting for Health on maximising the use of the NHS Care Record for research. It has simulated how clinical trials and large observational studies could draw on the NHS infrastructure, and will report shortly.

37. The Secondary Uses Group set up by the Care Record Development Board to advise on the ethical use of patient data and how the potential for research, statistics and management can be realised without compromising confidentiality or security is due to report shortly.

Conclusion

38. There is no room for complacency in a large and complex change programme that aims to achieve major and lasting improvements in patient safety and patient care. The supporting IT systems will process often intimate information about people and there needs to be a programme of continuous appraisal and improvement. The Department of Health intends to establish a National Information Governance Board (NIGB) answerable to the Secretary of State for Health, to provide a single authoritative source of monitoring, oversight and advice on the use of information in health and social care. The NIGB will review compliance with the NHS Care Record Guarantee and report annually to the Secretary of State. With increased availability of patient information, it is important to safeguard access and to retain the confidence of the public. The NIGB will prevent complacency by adopting and maintaining high standards and by being ever watchful and in touch with public perceptions.

April 2007

APPENDIX 37

Memorandum submitted by the Foundation for Information Policy Research

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 were asked by the adviser to the Home Affairs Committee to submit evidence on the large strategic issues of concern to the general public raised by the numerous public and private databases and forms of surveillance with a direct relevance to the work of the Home Office, including "the databases being developed by the Department of Health and the DfES for use in the fight against crime".

We would like to make the following points.

1. The UK does a lot more surveillance than other countries, especially when it comes to CCTV. This raises, at the very least, the question of whether the public money invested in these systems yielded a satisfactory return. In the case of CCTV the answer appears to be no: although CCTV is effective at reducing crime in car parks, where there are restricted exists, the evidence does not support its effectiveness elsewhere.[230]

2. The origins of the overinvestment appear to be as follows. The Criminal Justice and Public Order Act 1994 allowed local authorities to establish CCTV systems in order, inter alia, 'to promote the prevention of crime'. The current government started off well enough in 1997 with its 'Comunities that Care' initiative, under which local community leaders meet and suggest neighbourhood initiatives that would in their opinion reduce crime—which might include anything from better street lighting to improved sports and play areas. However, this appears to have become entangled with the CCTV initiative with the result that instead of subsidising "initiatives that would make your neighbourhood safer", the Home Office has been subsidising "initiatives that would make your neighbourhood safer using CCTV". As a side-effect, the "Communities that Care" initiative appears to have languished, or at least been much less effective than the US pilots on which it was based. The Committee should therefore consider not just the waste of public funds but also the opportunity costs—the better crime-reduction initiatives that were crowded out.

3. Once these lessons are learned, we may expect that in future there will be less CCTV surveillance. However there will still be some, and the Committee should next consider the issue of access to and processing of stored image data. In the past there have been some notorious abuses (including operators selling images of people having sex). The Data Protection Act 1998 empowers the Secretary of State to order "assessment" of processing operations that "appear[] to him to be particularly likely—(a) to cause substantial damage or substantial distress to data subjects, or (b) otherwise significantly to prejudice the rights and freedoms of data subjects" (Section 22(1) DPA98). Justice has called for data matching CCTV cameras and facial recognition software in particular to be designated as 'assessable processing. Unfortunately no such order has been issued.

4. We would like to raise an important point that we believe has been overlooked. Strategic issues raised by CCTV (and other forms of surveillance) are not limited to privacy, but extend to equality of arms in both criminal and civil cases. It is much easier for the police to get access to CCTV images to prove guilt than it is for a citizen to get access to establish an alibi; and in civil disputes involving (for example) disputed ATM withdrawals, a customer in dispute with her bank will typically find it impossible to get the relevant CCTV images.

5. We suggest that committee members read David Brin's book *The Transparent Society*, which argues that given the dramatically falling costs of data acquisition, storage and processing, we face a choice of two futures: one in which the government knows everything about its citizens who are disempowered and alienated as a result, and an alternative in which citizens can also observe the rulers (and each other). Brin argues for the abolition of most forms of privacy; he suggests not only that anyone should be able to read anyone else's bank statements, but even that anyone should be able to tap anyone else's phone. While Brin takes an extreme position to make his readers think, his position contains a kernel of truth. A world in which the spooks know everything, the police know almost everything, the banks and credit reference agencies know an awful lot, and the citizens know very little, will not be the same as the Enlightenment vision of a democracy of citizens equal under the law.

6. Parliament's historic attempt at balance was the Freedom of Information Act, which made the Information Commissioner responsible for encouraging the flow of information to the ruled about the rulers as well as for limiting the flow to the rulers about the ruled. This is inadequate for two reasons. First, there are constant pressures on governments in the other direction, so the balance is steadily eroded. Second, such a dispensation is essentially a centralising one. State action displaces private action: only the state has the information needed to act.

---

[230] M Gill, A Spriggs, *Assessing the Impact of CCTV*, Home Office Research Study 292, February 2005; see also their other publications at www.perpetuitygroup.com

7. For example, the Government has struggled for years to make the Child Support Agency into an efficient vehicle for recovering a certain kind of civil debt, namely alimony. In the process it has caused much misery. We suspect the solution must be to give citizens better mechanisms to recover civil debts of all kinds. Thus a divorcee seeking to enforce a court judgement should be able, by court order, to track down a fugitive partner, identify his registered assets from bank accounts through motor vehicles to real property, and seize what is due to her. Similarly, as technology makes it simple to keep CCTV images forever rather than just for a week, someone wishing to establish that they did not make a disputed ATM transaction, or to establish an alibi in a criminal matter, should be able by order to access the relevant images.

8. Transparency and equality of arms would go a long way in ensuring that public support for surveillance is retained in the long term. The same applies to access to databases; information sharing between public sector bodies and private agencies will be undermined if the exercise is seen as favouring big companies against small firms or individuals, or the strong against the weak generally.

9. Matters will be even worse if large quantities of public-sector data start flowing to the private sector; government datasets are notoriously inaccurate, and if they start being used by credit reference agencies and banks in lending decisions, then innocent people will be harmed. If, at the same time, more and more government departments start using credit reference agency data, there is a clear risk of positive feedback loops whereby some wrong information on a citizen, whether entered accidentally or maliciously, contaminates a number of public and private databases, making some poor citizen's life a misery. In a world of pervasive and growing "identity theft" this is not acceptable.

10. We put the term "identity theft" in parentheses because we don't agree with it. Ten years ago, if someone went to the Midland Bank, pretended to be me, borrowed £10,000 and vanished, that was the crime of impersonation; it was the bank's problem rather than mine. Now it's called "identity theft"—supposedly it's not the bank's money that's been stolen but my identity. This suits the banks as it help them dump fraud liability on customers, and it suits the Home Office as they think it will help them sell identity cards.

11. But from the point of view of data protection, the problem is that credit reference agencies knowingly pass on false information about the "victims" of "identity fraud" even although they know that the victims have nothing to do with it. When challenged, the agencies say that they are simply holding this data on behalf of the banks. This is untrue as in law they are the data controllers, and by passing on false information they break the fourth data protection principle. They are also committing a civil libel. The Information Commissioner should be ready, on application from a victim of "identity theft", to issue an enforcement notice against the agencies committing the defamation. Unfortunately, successive Information Commissioners have proved reluctant to act. That must change if more public-sector use is to be made of agency data (and indeed in any case).

12. On the topic of "identity", a controversial bundle of issues centre on the ID card system and the identity register that will stand behind it. FIPR gave evidence to the Committee on this topic in 2004; we refer the Committee to that evidence and also to the LSE report warning about the project's likely costs[231]—which seems more prescient with every new cost escalation. We remain deeply sceptical about this project. Recent research[232] also strongly suggests that the obsession with identity since 9/11 has damaged the fight against fraud and money laundering; "follow the man" and "follow the money" are not perfect substitutes, and an overinvestment in the first has caused the neglect of the second.

13. The Committee asks about the potential abuse of private databases by criminals. Honourable Members should also consider the abuse of public sector databases; there has been considerable concern, from the public to senior police officers, about potential abuse of the proposed identity register. It is already the case that public sector databases are unlawfully accessed on a regular basis by private detectives and others, especially when they wish to trace people.

14. Two members of FIPR's Advisory Council were involved with the BMA in an experiment in 1996 to determine the extent of abusive access to NHS data. Staff at the North Yorkshire Health Authority were trained to detect and deal with false-pretext phone calls, by logging calls requesting personal data and calling back to a number found in a phone book rather than to the number given by the caller; this simple authentication mechanism revealed some 30 false-pretext calls a week. The BMA asked the Department of Health to extend these operational security measures throughout the NHS; its response was to order the NYHA to cease and desist. No doubt many people have been traced, and/or had their personal health information compromised, since then.

15. The new Population Demographics Service in the NHS will make it easy for any NHS staff member to trace anyone in the country, including ex-directory numbers (although it is possible to opt out of PDS, you then cannot use Choose and Book or electronic prescriptions). The identity register, if built, will no doubt be used for similar purposes. The Police National Computer has long been abused by corrupt or careless officers despite a substantial audit resource and frequent prosecutions; public-sector databases accessed by staff under less discipline, who are audited less rigorously, and who work for organisations that care less about security, will likely be abused more.

[231] *The Identity Project—as assessment of the UK Identity Cards Bill and its implications*, LSE, June 2005; at csrc.lse.ac.uk/IDcards/identityreport.pdf

[232] *Closing the Phishing Hole: Fraud, Risk and Nonbanks*, Ross Anderson, Federal reserve Santa Fe Conference, 4–6 May 2007; at www.ross-anderson.com

16. Thus, at present, the state's ability to trace people is made available to private individuals through unregulated and largely unlawful means. This facilitates various sorts of harm, from the harrassment of celebrities to intimidation of witnesses and vengeance against former partners' lovers. We propose instead that there should be properly regulated mechanisms for tracing individuals and assets. This should remove much of the demand from private investigators for access to such material. Draining the swamp will surely be better than giving a short jail sentence to the occasional crocodile.

17. The Committee asks about Home Office use of health and education databases. FIPR wrote a report *Children's Databases—Safety and Privacy* for the Information Commissioner in 2006.[233] There we documented the government's plans to link up databases with information on children, including NHS, social work, police and education systems. A key driver is the Home Office belief that future delinquents and offenders can be identified and targeted for early intervention. We are deeply sceptical about this; it is extremely likely that the costs will greatly outweigh any benefits.

18. The Committee asks about 'Profiling'; we'd suggest it consider the analysis set out in our report. It is very hard to predict which children will offend, and the attempt carries a serious risk of stigmatisation, so that predictions can become self-fulfilling. Many young people successfully overcome multiple disadvantages, such as a bad neighbourhood, a single-parent family and poor health; marking all multiply-disadvantaged youths as "likely to offend" is unjust. Equality activists have long talked of the "offence" of "driving while black"; the risk of profiling is that young people in future may be pulled over for "driving while having more than 60 points on the ONSET system". If vulnerable young people are repeatedly stopped by the police, or treated like suspects rather than witnesses whenever they come to attention, then they can easily be driven to rebellion and criminality.

19. Quite apart from the law-enforcement aspects of child surveillance, there are grave doubts about its effectiveness in social care. There is a shortage of effective interventions, with Communities that Care and Sure Start having been largely ineffective; there is a serious risk of losing the confidence of social workers, teachers, doctors and other professionals, and of compromising public confidence in the confidentiality of health and social services. (This trust has proven therapeutic value.)

20. In short, the costs of widespread information sharing on children appear to greatly exceed the benefits. Even if officials argue that they can predict from surveillance who'll offend, there are much easier ways to identify troublesome kids (just ask the teachers); but it's not easy to do anything about them, and it's not Home Office turf anyway. It's pointless to do surveillance and not be able to act on it, and action is the hard part. Furthermore, a number of the proposed information flows are contrary to European (and thus UK) law.

21. Another example of police use of health data goes back to 1996, when there was a tussle between the government and the BMA over granting the police access to the Prescription Pricing Authority database. This was sought with the argument that the police needed to track down the small number of doctors and nurses who abuse their ability to prescribe opiates. Eventually the BMA decided not to fight the issue, and conceded police access. Yet Dr Shipman kept on murdering his patients for several years after that. The Committee might care to ask ministers how this happened. This may help bring home that simply sharing data between government departments and agencies does not by itself mean that anything useful will be done with it. As well as the data, there must be mechanisms, systems and above all incentives; for the police, the PPA data may have been "nice to have" but trawling it was presumably not a priority as they didn't know that a Shipman existed. Perhaps if the GMC had been assigned the surveillance task, Shipman would have been caught sooner.

22. The committee asks about "Existing safeguards for data use and whether they are strong enough". The brutal answer is that UK data protection law has always been not only weak but defective. This is not a party political issue; data protection acts introduced by both parties have equally failed to give effective force to European treaties and law. This is explored in detail in chapter 7 of our report on children's databases.[234] The effect in healthcare is that while everywhere else in Europe governments consider it necessary to get patient consent for secondary uses of health records, here in the UK it is considered sufficient to offer some limited (ineffective) patient opt-out from some of the applications. The risk is that a future European law challenge will undermine NHS business processes that by then might be expensive to change. (This matter is currently being considered by the Health Committee, which is due to report in July.)

23. The Committee asks about monitoring of abuses. As we remarked above, the PNC is the one public-sector database where a real effort is made to catch abusers, and even that doesn't stop abuse. In the NHS, privacy breaches are not reported to patients but to "Caldicott Guardians", typically senior managers who have every incentive to cover up problems in the absence of clear evidence of actual harm. The only way to get the incentives right is to notify patients, as is done in many other countries. Indeed FIPR believes that the UK should have a security breach disclosure law, as exists in most US states; any organisation suffering a breach of systems security should be compelled to notify all data subjects whose information may have been affected. This is desirable for many reasons other than privacy; for example, people whose credit cards

[233] Available from www.ico.gov.uk and from www.fipr.org

[234] See also Professor Korff's testimony for FIPR to the Health Committee enquiry into the Electronic Patient Record.

have been compromised should be told so that they can have them reissued.[235] (There is an EU proposal for a directive on security breach notification, but it's limited to telecomms; this is one area in which the UK legislator could usefully go farther and faster than Brussels.)

24. FIPR also testified to this Committee in 2006 about forensic problems caused by the growing volumes of data seized nowadays and police inability to cope. We mentioned that Operation Ore had caused particular problems by its extravagant resource consumption. Recent revelations about the incompetence (to put it at its most charitable) of that operation are deeply disturbing: it appears that about two thousand people were raided by the police during 2002–06 on suspicion of having downloaded child pornography when in fact they had simply been victims of credit card fraud. Security breach disclosure laws will help prevent a repetition of this (though many other things are needed too, from better police forensics through to punishment of the culprits in that particular case).

25. Action is needed to make the Information Commissioner's Office more effective and to make proper penalties available for abuse. First, the ICO has always been lacking in technical capability, which has undermined its credibility. Second, the proposed changes to data protection law, agreed by the ICO and the Ministry of Justice, provide for (short) prison terms to be available for private detectives and others who gain improper access to data, but not for the data controllers who give them this access. This is also unsatisfactory. In fact, we think that the ICO needs a radical rethink; Parliament should consider the proper allocation of the regulatory tasks currently performed by the ICO, the various surveillance and intelligence commissioners, and the IPCC. What governance structures are needed to ensure that official access to information is not abused in the information age? What laws or institutions are needed to overcome or sidestep the civil service opposition to privacy and freedom-of-information laws that has undermined the ICO to date?

26. In summary, we're deeply sceptical about the notion that pervasive surveillance will solve social problems. It's been tried for over a dozen years, and we have yet to see the evidence that Britain has gained, say by comparison with Germany where privacy laws are better enforced. The huge investment in CCTV looks like a mistake, and spending billions more on identity registers, children's databases, ANPR, and other mass surveillance systems, is foolish. The vendors of these systems have mostly failed to make a case on costs and benefits.

27. There is also a deep political question about the relationship between the citizen and the state. A frequent objection to the ID card project has been that many people prefer the "British way", whereby the policeman shows his warrant card to the citizen, rather than the "German way" in which the policeman imperiously demands the citizen's *Ausweis*. Other mechanisms of surveillance and control will carry similar side-effects. We won't be able to predict them all in advance, but legislators should still have some guiding principles.

28. We'd therefore suggest that the Committee try to develop a vision of how citizens relate to the state, and to each other, in an information society. How should society regulate access to the masses of public and private sector data that are gathered, or that can be used for, surveillance? If there is going to be a "British way", what should it be?

May 2007

APPENDIX 38

Memorandum submitted by Experian

About Experian

Experian is a global leader in providing analytical and information services to organisations and consumers to help manage the risk and reward of commercial and financial decisions. Combining its unique information tools and deep understanding of individuals, markets and economies, Experian partners with organisations around the world to establish and strengthen customer relationships and provide their businesses with competitive advantage. For consumers, Experian delivers critical information that enables them to make financial and purchasing decisions with greater control and confidence. Clients include organisations from financial services, retail and catalogue, telecommunications, utilities, media, insurance, automotive, leisure, e-commerce, manufacturing, property and government sectors.

Experian Group Limited is listed on the London Stock Exchange (EXPN) and is a constituent of the FTSE-100 index. It has corporate headquarters in Dublin, Ireland, and operational headquarters in Costa Mesa, California and Nottingham, UK. Experian employs more than 12,500 people in 34 countries worldwide, supporting clients in more than 60 countries. Annual sales are $3.1 billion (£1.7 billion/€2.5 billion).

[235] See Professor Anderson's testimony for FIPR on this topic to the Lords' Science and Technology Committee enquiry into Personal Internet Security.

1. Executive Summary

1.1 The purpose of the paper is to provide the Home Affairs Committee with background to what a credit reference agency does to assist with its inquiry.

1.2 A credit reference agency (otherwise known as a credit bureau) does not make any lending decisions in its own right nor does it express any opinion as to an individual's ability to repay a loan. Rather it provides factual data and tools to lenders for this purpose. Lenders will make their decision based on information provided by the consumer, information obtained from a credit reference agency (which is obtained with the consumer's consent), information from other sources and most importantly, against that particular lender's underwriting criteria.

1.3 Information held by a credit reference agency largely consists of publicly available records, such as the electoral register, county court judgments and bankruptcies. Alongside this it holds information relating to credit applications and credit accounts provided by lenders, with the consent of the consumer. By bringing this objective information together lenders can make accurate, responsible decisions about an individual's ability to repay a loan.

2. Data Protection within Experian

2.1 It is a key strategy for Experian to position itself with consumers and its clients as a trusted custodian of personal data and an acknowledged leader in the field of compliance, data protection and data sharing. Its dedicated Regulatory and Consumer Affairs team is charged with this responsibility across Experian.

2.2 Experian facilitates the sharing of data through a secure database repository where data are obtained, stored and accessed strictly in accordance with relevant legislation and codes of practice governing the use of shared data.

2.3 Experian operates in a highly complex and regulated environment. The Data Protection Act 1998 governs the processing of personal data both by Experian clients and by Experian itself. There is other legislation governing the use of specific datasets—The Representation of The People Act controls the use of electoral register data.

2.4 As a Credit Reference Agency Experian is also licensed by the Office of Fair Trading under the Consumer Credit Acts 1974 and 2006. Consumer complaints can be directed to both the Information Commissioner's Office and Financial Ombudsman Service.

2.5 Experian is committed to achieving the highest possible levels of data accuracy, security and integrity. Its Regulatory and Consumer Affairs function works closely with regulators, including the Office of Fair Trading and the Information Commissioner, to ensure that all procedures, products and systems are carried out and developed to their satisfaction and within the appropriate legal framework.

2.6 Commitment to compliance and data protection is further demonstrated through Experian's active participation on government consultative groups, industry trade bodies and associations, together with direct client involvement to increase compliance and data protection awareness.

2.7 Equally Experian is committed to its consumer-facing obligations as a Credit Reference Agency. Its Consumer Operations department of over 200 people is dedicated to working with consumers and suppliers of their data to ensure its accuracy. In tandem with this service, Experian liaises with the media, government, money advisors and consumer organisations to promote transparency in terms of what personal information is held and why and how it is used.

2.8 This submission expands on the role Experian plays as a credit reference agency.

3. Credit Referencing in the UK—The Use of Personal Information

3.1 The UK has three consumer credit reference agencies. Their databases bring together data from many different sources—public, proprietary and self-reported by consumers—to provide the basis for informed and timely business decisions by their clients. These decisions are primarily around credit applications, but increasingly relate to authentication checking—confirming the consumer is who they claim they are, which is critical for lending decisions and indeed is required by Money Laundering regulations.

3.2 The credit reference agencies provide comprehensive information on the credit status of individuals by combining publicly available records with credit account details received from many hundreds of credit grantors.

3.3 When consumers seek financial services, they provide the financial service provider with information on their financial position. As part of the process of underwriting a consumer's application, the majority of providers, with the consent of the applicant, utilise the facilities of one or more of the UK credit reference agencies. These supply the financial service provider with reliable credit performance data from other financial institutions, relating to the consumer. The credit reference agency does not disclose the origin of such information to the provider.

3.4 The consumer benefits from choice and competition across a wide range of financial services, which has been made possible by the innovative and technologically advanced collection, use and delivery of information. The credit reference bureaus provide up-to-date and comprehensive information to a wide range of consumer facing organisations, enabling them to offer swift and discrete decisions in shops, banks and a range of other organisations, face-to-face and on the telephone or via the internet.

3.5 Consumers benefit from the knowledge that their information is provided and assessed in an understandable and controlled format and that they have the right to access their records at any time, and ensure the information is correct. They also have confidence that their data may not be accessed by unauthorised persons and that it is protected by law under the provisions of the Data Protection Act 1998.

3.6 Data sharing in the UK is governed by the Principles of Reciprocity—as agreed and policed by the Steering Committee on Reciprocity (SCOR)—as well as being subject to all the legislative requirements relating to the processing of personal data.

3.7 SCOR is an industry body consisting of representatives from the British Bankers Association, Finance and Leasing Association, Council of Mortgage Lenders, Consumer Credit Trade Association, Mail Order Traders Association, APACS, Consumer Services Association and Consumer Credit Association, together with representatives from the three UK credit reference agencies. Credit reference agencies are not therefore able to determine unilaterally how shared personal data may be used.

4. The UK Credit Market

4.1 The UK credit market is the second largest in the world after the USA, with the majority of the adult population holding a range of financial products, from a wide variety of organisations, as a matter of course.

4.2 Competition to satisfy the demand in the UK is increasingly fierce. Many consumers move from lender to lender, taking advantage of opening offers and moving on to the next attractive deal when the offer expires.

4.3 At a time of record levels of UK debt, lenders are more reliant than ever on full bureau information to ensure that the new-to-organisation applicant can be identified and their financial position and stability understood in order to make credit or financial service decisions. Legitimate and transparent access to data has been fundamental to the development of this competition.

4.4 Lenders use credit bureau data, inter alia, for risk assessment and affordability decisions to ensure consumers are offered the most appropriate product for their specific requirements.

5. Data Protection, Privacy and Data Security

5.1 Lenders search the databases at credit reference agencies with the full knowledge of the applicant. A standard notification and consent wording agreed with the Information Commissioner is now being widely used by banks, credit card issuers and similar organisations.

5.2 Other clauses advise the customer whether records of applications and information on the performance of credit accounts are lodged with credit reference agencies and made available for the purpose of the prevention of over-commitment and fraud.

5.2 Only those consumer records on which consent to share the data is given are held on the credit bureau.

5.3 Extensive client veracity checks are conducted before a financial services provider is permitted access to a credit bureau's records. Ongoing monitoring is also carried out to ensure patterns of client usage are consistent.

5.4 Physical data security is critical to Experian, with a multi million pound investment having been made in a purpose built data centre. This is backed up by strict data access controls and protocols overseen by a dedicated Information Security function. All Experian employees and clients who require access to Experian systems and information are individually authenticated before any information is provided. Rigorous access controls ensure that information is only provided to authenticated users based on their authorised job function/responsibilities.

5.5 In addition to compliance with the Data Protection Act, credit reference agencies work to a number of other regulatory requirements, codes of conduct and guidance notes such as the industry-backed Guide to Credit Scoring and the Information Commissioner's Guidance Notes on Credit Referencing and Defaults.

6. Benefits of Data Sharing

6.1 The UK financial services market is highly sophisticated, competitive and delivers real choice and benefit to both the consumer and the economy. It has grown and developed as UK financial services companies have developed through competition. That competition has been possible because of the open nature of the UK market and the increasing sophistication of UK consumers.

6.2 Barriers to entry for financial services providers are low and the availability of information from shared databases at credit reference agencies enables real competition to thrive. It also makes it possible for lenders to lend more responsibly and monitor account behaviour on an ongoing basis.

6.3 The benefits and value of the UK model are acknowledged in the work undertaken annually by the World Bank in its "Doing Business" survey, see http://www.doingbusiness.org/, which identifies the UK as the top-ranking country in which to obtain credit based on the balance between legislative protection for consumers and lenders together with the breadth of information in the credit reference agencies. It considers that a functioning and effective credit industry is a vital contributor to economic stability and growth in GDP.

6.4 The Competition Commission has also recognised the pro-competitive impact of the provision of shared access to consumers' payment data in its recent report on home collected credit.

7. Working with Consumers—General

7.1 As a credit reference agency Experian has statutory obligations under both the Data Protection Act and Consumer Credit Act to provide a consumer with a copy of their credit report and to help them deal with any queries on this report, if necessary liaising with lenders and other third parties on their behalf.

7.2 Over the past 12 months Experian has provided over 1.5 million new credit reports to consumers and a further three million repeat reports through its on-line credit report membership and monitoring service. Its Consumer Services team helped over 900k consumers with questions on their credit reports.

7.3 Experian takes its consumer obligations much further than this and works closely with consumer groups, such as Citizens Advice, Which? and the National Consumer Council, and with money advice organisations like the Consumer Credit Counselling Service and National Debtline, providing free credit reports to people who are receiving free debt counselling.

7.4 Similarly Experian's clients are encouraged to be as forthcoming as possible about the role credit reference information plays in their decisions to make sure consumers get accurate and helpful information when they need it. Experian also works very closely with all the relevant lending trade associations on a variety of issues and initiatives.

7.5 Its Consumer Affairs team regularly provide material for publications and contribute extensively to all forms of media, including television and radio, to ensure that consumers are aware of their rights in this area.

7.6 Experian's free booklet, The Credit Reference Agency Explained provides an overview of the credit reference agency's role and its "Credit Crossroads" leaflets provide advice and guidance around financial issues and "life events". These are distributed through citizens advice bureaux and other consumer advice centres.

7.7 Each year, the Consumer Affairs team spend considerable time talking directly to consumers at exhibitions such as the conferences of Citizens Advice, The Institute of Money Advisers, Money Advice Scotland, the Trading Standards Institute as well as at consumer events like the Ideal Home Show and BBC Good Homes Show.

7.8 At a policy level Experian is involved in several consumer education and financial capability projects, including those led by the Financial Services Authority, the Office of Fair Trading and the Personal Finance Education Group.

7.9 Most recently in 2006, Experian launched a resource pack for teachers, *Getting Credit: A Beginner's Guide*, to help them deliver numeracy and literacy lessons around the theme of applying for, getting and managing credit. Additionally support is provided to the Young Consumers of the Year competition, giving the schools that take part information about consumer credit and helping set questions about the process for granting credit.

8. Working with Consumers—Victims of Fraud Service

8.1 Since 2003 Experian has provided a dedicated support service to consumers who have been victims of identity fraud. During this time, assistance has been given to over 15,000 identity fraud victims. There are now on average 100 victims of fraud contacting Experian's Victims of Fraud team each week.

8.2 This free service was introduced to offer consumers a single point of contact and to act as intermediary in the restoration of a consumer's accurate credit history. By acting on a consumer's behalf and by co-ordinating any necessary activity the Experian service significantly reduces the amount of time it would normally take an individual to restore his or her credit history.

8.3 Once Experian has established that an individual is a true victim of fraud and their identity has been fully authenticated, they are provided with the following:

— A dedicated case worker (with a freephone number), who will give general and ongoing advice on identity fraud as well as dealing with the specific problems being experienced by that individual and helping to liaise with lenders on their behalf.

— A free copy of their credit report along with copies of Experian's consumer advice leaflets—*Your Credit Report Explained and Identity Fraud Explained*.

— A discrete password which is added to their credit report which ensures lenders are alerted to the fact that an individual has been an ID fraud victim and should therefore request the password prior to proceeding with an application for credit.

— Information about and referral to CIFAS (the UK's fraud prevention service) for Protective Registration.

— Free 12 month membership Experian's credit report monitoring service, CreditExpert.

9. Conclusion

9.1 The UK model enables the consumer to shop around for the best deal secure in the knowledge that lenders are able to see the most up to date information about them and make the best possible decision. Consumers are no longer limited to taking products from the organisation with which they already have a relationship because other do not know enough about them. As a result, healthy competition has driven down the cost of credit to consumers and resulted in wider choice.

9.2 The macro and micro economic benefits of this are acknowledged in the DTI White Paper in 2003—*Fair, Clear and Competitive—The Consumer Credit Market in the 21st Century*, which opens with the statement:

> "Consumer credit is central to the UK economy. Economic stability based on sound fundamentals is bringing rising prosperity, record employment and low interest rates, all underpinning increased demand for credit. For most, credit cards and other secured and unsecured lending provide people with greater control and flexibility when managing their finances—collectively benefiting the economy A competitive and efficient financial sector, of which the consumer credit market is an important part, is essential to raise the level of economic growth in the UK economy."

9.3 The World Bank makes it clear that central to the success of the UK consumer credit market is the effective and competitive credit bureau regime in the UK.

9.4 At the same time, the consumer's rights under the Data Protection Act to obtain a copy of the information held about them (and to get it queried and/or corrected if it is incorrect) gives them the security of knowing what information was used to make that decision and critically, who has been looking at it. This is because every access is required to leave a footprint visible to that consumer showing when and by whom their credit report was searched.

9.5 Credit referencing in the UK is transparent. A credit reference agency provides a central and highly controlled repository of information that may be made available only with the consent of the data subject for purposes that benefit them, typically in accessing goods or services.

May 2007

APPENDIX 39

Memorandum submitted by the Loyalty Management Group

BACKGROUND SUMMARY OF NECTAR

Introduction

1. The Home Affairs Select Committee has invited Loyalty Management Group (LMG), the company that owns and operates the Nectar Card, to provide oral evidence to its inquiry into "A Surveillance Society?" on 7 June 2007. To assist the Committee in terms of background information and what we understand the Committee may be interested in; this written summary provides a detailed overview of how Nectar collects, uses and protects data on the individuals that participate in the Nectar loyalty programme.

The Nectar Programme and How it Operates

2. Nectar is a coalition loyalty programme. It consists of retailers and service companies that sign up to Nectar and offer Nectar Points to consumers. Currently there are 15 Nectar partners, each with sector exclusivity in the area in which they operate. This means, for example, that there is only one grocery supermarket, one petrol retailer, one department store, or one car-hire company in each sector participating in Nectar at any one time.

3. Nectar is an entirely voluntary scheme which consumers actively decide to join. These consumers are called "Collectors". Collectors earn Nectar points from the retailers and service companies. Collectors normally earn two Nectar Points for every £1 spent, although this differs in a limited number of cases (eg

the rate is one Nectar Point for every one litre of fuel from the petrol retailer). At the lowest level, 500 points is equivalent to a reward worth £2.50 to collectors. This equates to 1% of the money spent by Collectors on collecting their points. This benefit level can rise to 5% depending on where Collectors redeem their points. Collectors have a variety of options when they want to redeem points, which range from money-off shopping through to booking flights, days out at theme parks and free cinema tickets.

4. Since the launch of Nectar in September 2002 to May 2007, Collectors have redeemed over £800 million worth of rewards.

Collecting Data

5. Nectar collects information for two basic purposes:

(i) *Operational* ie to have Collectors' contact details and to operate their Nectar account by adding and deducting Nectar Points from Collectors' accounts as they collect and redeem their points.

(ii) *Marketing* ie to identify the shopping behaviour of Collectors so that Nectar and the partners in the programme can send Collectors offers that will be of interest to them. Information may also be analysed for internal purposes eg to validate the benefits a partner has gained from participating in Nectar.

Nectar Collects

6. Basic registration information for all Collectors collecting points on the account (name, address, phone number, e-mail address) and security information (date of birth and mother's maiden name or other memorable word); and basic lifestyle information (how many people live in the household, how many are under 18, number of cars in the household).

7. Shopping transaction information: where the Collector has shopped, on what date, total value of goods purchased. Nectar does not know the individual details of goods which are purchased. (For example: the data collected only tells Nectar Joe Bloggs shopped in the Westminster branch of Sainsbury's at 10 am on 4 June 2007, spent a total of £50 and is to be issued 100 points).

8. LMG would like Collectors to be engaged fully with Nectar by collecting and redeeming points and, if they choose to, by benefiting from the rewards and offers provided by Nectar. In order for Nectar to achieve this aim, it is paramount that it develops and maintains a high level of trust with Collectors, and a fundamental element of that relationship is that Nectar is openly transparent with how that data is used.

9. Partners in Nectar are only able to access data on their own customers and Nectar will carry out analysis on those customers for partners who wish to carry out marketing targeted at a particular set of their own customers eg BP may wish to make a particular offer to its customers who live within a certain radius of a petrol station. Nectar undertakes regular direct marketing communications with Collectors (eg its quarterly points update mailing) and partners can indirectly access Collectors who are not their customers by including an offer in those communications; if a Collector takes up that offer, he or she will then, of course, become a customer of that retailer or service company.

10. Nectar has established an internal code that applies for the benefit of the Nectar "coalition"—what we call our "database principles". These are included in all Nectar's contracts with companies which issue Nectar Points and set out the access that they are permitted to Nectar's data and also include some important safeguards for Collectors (eg Nectar has the right to refuse access to stop excessive communications). Nectar's success depends on gaining and maintaining the trust of Collectors and these principles are an important element of this.

11. Nectar also carries out specific marketing campaigns e.g. one that is very popular with Collectors is the offer sent when a collector has moved house, including a map of their new neighbourhood showing the nearest places they can collect Nectar Points and with bonus Points offers that can be used there.

Privacy and Data Protection

12. It is a requirement of the Data Protection Act that everyone from whom data is collected is made aware of the information on them that is collected, what it will be used for, and to whom it will be disclosed. This must be done at the time the data is first collected. Nectar's "Policy on Privacy and Data Protection" appears prominently wherever Nectar collects data eg from registration forms and the website.

13. Safeguarding Collectors' data is essential to Nectar's business and to Nectar partners. Unless Collectors have the confidence of knowing that their data is secure with Nectar, they will stop engaging with the programme or "de-register". Even if there were no legal requirements, this is the most powerful underlying reason for Nectar to ensure that its data is kept as secure as possible.

14. However, there is another important element, which is a requirement of Nectar's partners. It is equally integral to their customer service, business model and wholesale reputation that any personal data is kept secure. In short, if they did not have confidence that Nectar could protect this information, they would not participate in the Nectar scheme.

CONCLUSION

15. Nectar's primary business asset is data. It therefore has a fundamental business need to ensure that its data is collected, held, used and disclosed in a way that complies not only with legal requirements but meets and exceeds best practice. Nectar relies on the continuing trust of Collectors and an important element of this is that they are confident that their data is secure with Nectar and that Nectar will handle their data properly.

16. The underlying aim for Nectar and its partners is to understand the needs and wishes of Collectors when they go shopping. Through the collection of data Nectar is able to provide a more detailed offering to suit the tastes of individual Collectors. The Collectors and their interests are at the heart of our business model.

17. In summary, it is Nectar's number one priority to safeguard any data that Collectors voluntarily choose to share with us. To fall short of providing a high level of security would damage the reputation of Nectar and would result in Collectors signalling their disapproval of Nectar through ceasing to participate in the Programme. To avoid this, we ensure, and will continue to ensure, that Nectar data is safeguarded by stringent security.

June 2007

APPENDIX 40

Memorandum submitted by Randal Gainer, Partner, Davis Wright Tremaine LLP

EXECUTIVE SUMMARY

1. The personal information and payment card data of millions of individuals in the United States have been obtained by thieves who have electronically penetrated commercial and government databases and have stolen laptops and other computer hardware. In the one-year period ending September 2006, criminals used such stolen data to commit fraud against more that eight million individuals in the US Data breach notice laws in the US have exposed the breadth of this problem but have not motivated data controllers to implement adequate data security measures. New laws that are currently being proposed and adopted in the US will shift costs incurred due to data thefts from banks and individuals that currently bear those costs to organizations from which data are stolen if the organizations fail to implement certain data security measures. Mr Gainer advises businesses in the US regarding their legal duties to implement data security measures and to respond to data thefts. His testimony addresses the positive features and shortcomings of current US data breach notice laws and the new cost-shifting laws.

2. Mr Gainer is also co-counsel with lawyers from the American Civil Liberties Union in a lawsuit against the US National Security Agency regarding the NSA's interception of phone calls and emails of US persons and the NSA's data mining of telephone call records. He will testify about some of the issues raised by that case and will recommend certain restrictions on governments' use of data mining.

TESTIMONY

3. Thank you, Chairman Denham and members of the Committee for this opportunity to address some of the issues raised by the "Surveillance Society" report drafted for Commissioner Thomas. The report highlights serious threats to the privacy of residents of the U.K and of other countries, including the US I address here two issues raised by the report with which I have experience in the US: protecting the security of computerized consumer data and regulating government anti-terrorism surveillance. My testimony reflects my own views and not necessarily those of my firm, our clients, or my co-counsel at the ACLU.

The Positive Effects and Limitations of U.S. Data Breach Notice Laws

4. I represent businesses in matters that involve computer technology. In the last few years, I have assisted many businesses regarding thefts of electronic data. I would like to address some of the lessons we have learned in the US about statutes intended to protect consumer data from such thefts.

5. Theft of personal information is a serious problem in the US, as I understand it is in the UK In the one-year period ending September 2006, the last one-year period for which complete statistics have been reported, electronic data regarding more than 73 million individuals were stolen or lost in the US The information of at least 8.3 million of those 73 million persons was misused for fraud. Thirty-seven states in the US have enacted statutes that require entities that own or license computerized personal information about individuals to notify those individuals if unencrypted data about them is disclosed to an unauthorized person. The US Congress is considering proposed statutes that would apply across the US that would preempt these state laws and would require notice to consumers in all parts of the US in similar circumstances.

6. I understand that the UK has no similar data breach notice law, though some commentators have suggested that such a law should be adopted. A data breach notice law would be an important component of an effort to reduce the theft of consumer data. It would undoubtedly expose the extent of such thefts, just as such laws have done in the US Before California adopted the first US data breach law in 2003, reports of the theft of consumer data in the US were extremely rare. Now such thefts are reported daily. While there has likely been some increase in the number of such thefts between 2003 and today, it is not likely that such thefts began only after the notice laws were adopted. More likely is that organizations did not publicly disclose similar thefts that occurred before 2003.

7. Bringing the extent of data thefts into public view is important but it is not enough. One purpose of data breach notice laws is to expose companies and government agencies that fail to take available steps to protect data to negative publicity—with the hope that such exposure will cause them to improve their security measures. Another, important purpose is to permit potentially affected individuals and businesses to take defensive measures when individuals' data have been stolen. While the second purpose of data breach notice laws has been served by the statutes—individuals can monitor their accounts and banks and payment card companies can cancel accounts or change account numbers—the first purpose, improving security, has not been well-served by these statutes.

8. As part of my practice, I attempt to persuade business officials that they should take additional steps to protect consumer data. I regularly advise them that such preventive measures will be much less expensive than the costs of litigation, payment card association fines, or government penalties, all of which are possible if a data theft occurs. Very few businesses take adequate preventative steps to protect consumer data until after thieves have stolen such information. Business managers state that tight budgets generally do not permit expenditures for preventative security assessments and corrective measures.

9. Further, the deluge of data theft notices that have been issued since notice laws became effective in the US in 2003–04 has caused some consumers to ignore them. Something additional must be done.

10. I am aware that serious criminal penalties have recently been authorized in the UK for persons who steal private data. States in the US have even harsher criminal penalties available—and they impose serious penalties on data thieves when they police catch them. For example, a contractor's employee was recently convicted of stealing data from one of my clients. He was sentenced to four years in jail. Such potential criminal penalties have not, however, prevented the widespread theft of consumer data in the US.

11. A new approach is beginning to be adopted in the US. Last month, Minnesota became the first state in the US to adopt a law that permits financial institutions to recover costs related to data breaches from retailers that retain consumers' payment card data longer than necessary if the card data are later stolen. Financial institutions often have to replace payment cards when card data are stolen, which can cost up to $25 per card. In the past, US courts have held that banks may not recover those costs from retailers whose poor security contributed to a data theft. Five other US states are considering proposed statutes similar to the Minnesota law. AB 779, pending in California, would permit any owner or licensor of personal data to recover costs to send notices to affected individuals that are incurred after data are stolen from a business covered by California's data breach notice law.

12. Even these proposed new laws do not address a huge component of the financial costs of data thefts: pursuant to payment card association rules and standard payment card contracts, if a merchant accepts a fraudulent card for a transaction, the merchant will have to absorb the cost of the fraud. The cardholder is protected from having to pay such fraudulent charges by federal law in the US and by card issuers' policies. Card issuing banks are permitted to chargeback the losses to the merchant; therefore, unless the merchant has gone out of business, the issuer is protected as well. Merchants who get stuck with fraudulent charges typically pass those charges on to consumers by raising prices, ie, merchants adjust their prices to compensate for fraud losses. As is too often the case, it is the public that is penalized in the end.

13. If the best features of the recently enacted Minnesota statute and the other pending bills were combined, this outcome could be avoided. Any individual or business that incurs costs of any kind due to a data breach that was caused, in part, by another business's poor security measures should be able to recover those costs from the negligent business. Adequate security standards exist to determine whether a business has deployed adequate security, including the Payment Card Industry Data Security Standards and ISO 17799. Standards are not the problem. Failure to implement recommended security measures is the problem.

14. If such cost-shifting were authorized, negligent business would pay rather than consumers. Perhaps the risk of incurring such potential costs would motivate businesses to take additional steps to protect consumer data. Experience in the US shows that, until businesses (and perhaps government agencies) are threatened with paying for the costs of lax data security, many will fail to implement security measures that could prevent data thefts. Data controllers know that if a thief steals consumer data, others will bear most of the costs.

15. Some businesses do implement state of the art data security measures and they should be applauded. But the epidemic of thefts shows that data security is not the priority it should be.

16. Shifting the costs of data breaches has two additional benefits: it is fair—the negligent party pays—and it harnesses the power of economic incentives. Relying on mere shaming of data controllers has proven inadequate.

17. Cost-shifting could be adapted to the UKs regulatory approach to protecting data. The Information Commissioner could be authorized to order such cost-shifting if his investigation determines it is warranted.

The ACLU Litigation Against the National Security Agency

18. As you know, *The New York Times* disclosed the NSA's domestic surveillance program in December 2005. Two aspects of the NSA program were disclosed by the *Times* and by other media. One part of the surveillance program was the interception of emails and phone calls between US persons and non-US persons without either a criminal warrant or an order from the Foreign Intelligence Surveillance Court. The FIS Court is a specialized US court that considers government requests to authorize surveillance of foreign governments and terrorists. President Bush publicly admitted that he had authorized the phone call and email interception parts of the NSA program. The second aspect of the NSA program was the data mining of US persons' telephone call records to try to identify terrorists, which was also done without a warrant or FIS Court order.

19. The ACLU challenged the NSA program because the US Foreign Intelligence Surveillance Act, adopted in 1978 after politically motivated spying on US citizens by US intelligence agencies was exposed, requires domestic foreign intelligence surveillance to be conducted only as authorized by the FIS Court. The ACLU also claims that the NSA program violates US persons' free speech and due process rights. The ACLU challenged both aspects of the NSA program in federal court in Detroit.

20. I volunteered to help the ACLU and asked for help from other lawyers in our firm. More than a dozen attorneys in our offices have helped the very capable lawyers of the ACLU's national office with the litigation. We are doing that work *pro bono*. Such work by US attorneys is not unique. Others of my partners are representing prisoners at the Guantanamo Bay detention center. Lawyers from many other US law firms are similarly representing clients challenging US government actions that violate US and international law.

21. In addition to the ACLU lawsuit, more than 20 cases were filed in numerous cities across the US that challenged telephone companies' disclosure of call records to the NSA. Such disclosures are prohibited by US statutes in most circumstances and the statutes provide substantial financial penalties for each instance of unauthorized disclosure of call record data. The lawsuits against the phone companies were consolidated before a federal judge in San Francisco.

22. In the ACLU case, we obtained declarations from the plaintiffs—criminal defense lawyers, reporters, and scholars—that showed they could no longer communicate with confidential non-US sources without putting those sources at risk. The government did not dispute that evidence but sought to have the case dismissed on the grounds that it endangered state secrets. The government also claimed we could not show that the plaintiffs were actually targets of the program. Finally, the government argued that, if the court reached the merits, it should hold that Congress authorized President Bush to conduct the surveillance as part of the Authorization for Use of Military Force in Afghanistan or that the President has inherent authority, as Commander in Chief, to conduct the program.

23. In August 2006, Judge Anna Diggs Taylor held that the NSA had violated FISA and the First and Fourth Amendments to the US Constitution by intercepting US emails and phone calls without FIS Court approval. She rejected the government's state secrets claim about those aspects of the program because the government had publicly admitted them. She rejected the government's remaining arguments and ordered such surveillance to be stopped. Judge Taylor dismissed our data mining claims, holding that those claims were barred by the state secrets privilege.

24. Each side appealed. The Court of Appeals in Cincinnati suspended the injunction until it decides the case. Just before oral argument regarding the appeal on 30 January 2007, and just before Congress began hearings about the NSA program, the government announced that the FIS Court had approved the NSA program but that the government reserved the right to re-commence it at any time without FIS Court approval.

25. Judge Walker also refused to dismiss the lawsuits against the phone companies, which challenged the companies' disclosure of call records to the NSA. His decision is being reviewed by an appellate court in San Francisco.

26. A few weeks ago, former Deputy Attorney General James Comey testified to a Senate Committee that he and former Attorney General Ashcroft concluded in 2004 that the NSA program was illegal in its then-current form and that they had refused to sign a certification as to its legality. Mr Comey described an episode during which then Whitehouse counsel and now Attorney General Gonzalez sought to get Ashcroft to sign the certification while he was hospitalized for an acute illness. Mr Comey testified that President Bush agreed that unspecified changes should be made to the NSA program after numerous Department of Justice officials, including Mr Comey, Attorney General Ashcroft, and FBI Director Mueller, threatened to resign if the illegal program continued.

27. The cases regarding the NSA program are important for several reasons. First, it is critical that US courts reiterate the principle that even the President must abide by statutes enacted by Congress. The rule of law requires no less.

28. Second, it is important that the courts reject the President's misuse of the state secrets privilege. The rule of law cannot survive if the President can break the law, admit it publicly, and then invoke the state secrets privilege to prevent judicial review of his actions.

29. Finally, it is important that the courts limit the government's computerized searching of billions of telephone call records of millions of individuals, whom the government does not allege have done anything wrong. If such surveillance is to be conducted, court review and supervision should be required.

Data Mining of Government and Commercial Transaction Data

30. The "Surveillance Society" report discusses at pages 38–48 some of the reasons that unregulated government mining of personal data about ordinary citizens is objectionable. Other authors have described additional reasons that such government data mining should be strictly regulated.

31. There are at least six types of potential errors and abuses that may result from governments' counter-terrorism data mining efforts:

- Mistaken identity—a person with a similar name or other characteristics shared with a terrorist or criminal suspect may be misidentified as the target. This arises frequently with use of "watch lists" used to screen airline passengers.
- Faulty inference—information may be misinterpreted to draw an erroneous inference that someone is associated with terrorists when he is not.
- Intentional abuse—agents authorized to access data have performed checks for fees for private investigators.
- Security breaches—government data developed through data mining may be stolen or carelessly disclosed.
- Mission creep—systems justified to fight terrorists may be used for additional purposes, including law enforcement or increasing government control over individuals.
- Diminished trust—citizens may feel that they are under generalized surveillance, which will diminish their trust in government and inhibit their willingness to participate in lawful activities that may be misinterpreted, such as enrolling in pilot training.[236]

32. The last problem with data mining of consumer records, that it will heighten public distrust of government, is more ephemeral that the other potential abuses. It may, however, be the most important because it draws on individuals' unease about dramatic technological changes that have occurred in the last few years. Growing computer power and the declining cost of storing data make it practical for governments to store and search vast quantities of data. This, in turn, has decreased the "practical obscurity" that gave some comfort to individuals when it was impractical to collect scattered paper records and review them all. While there is still some potential obscurity that results from the massive volume of data available to governments, both from their own records and from commercial data aggregators, software search tools are rapidly improving, which is decreasing that obscurity as well.[237]

33. The threat to public safety has also changed. Threats are no longer posed primarily by hostile nation states. Terrorists, both those who are homegrown and those who infiltrate our borders, now threaten mass murder. Governments and individuals expect technology to be used to create actionable intelligence to identify terrorists and to prevent them from harming innocent people. US intelligence agencies' past failures to "connect the dots" have been universally criticized.

34. The ability to store vast amounts of data, the increasing ability to effectively search large databases, and the need to use all lawful means to prevent terrorists from carrying out their plans challenges policy makers to determine how to protect both privacy and security. Several technological tools can help and should be required:

- Anonymization—personally identifiable data in databases that are mined as part of counter-terrorism efforts should be anonymized. If a search produces a "hit," the specifically identified dataset can be de-anonymized. Anonymization should decrease individuals' concerns that every aspect of their lives is scrutinized.
- Access to data must be limited—permissioning rules for accessing the huge troves of government and commercial data that are aggregated for data mining should be built into system architecture and should be enforced.
- Immutable audit trails—each access to a database that contains personally identifiable data should create a log entry that cannot be changed. Such logs should be monitored to guard against intentional misuse of the data.

[236] Jack X Dempsey and Paul Rosensweig, *Technologies that Can Protect Privacy as Information Is Shared to Combat Terrorism,* 3–4, May 26, 2004, Center for Democracy and Technology.

[237] K . Taipale, *Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties,* in *Emergent Information Technologies and Enabling Policies for Counter-Terrorism*, Robert L Popp and John Yen, editors (Wiley Interscience 2006), 444–45.

35. Requiring privacy impact statements or "surveillance impact statements" for government surveillance programs, as recommended by Commissioner Thomas, may also help if a proposed surveillance project will be stopped or revised if an impact statement shows that the project will compromise individuals' privacy without producing results adequate to justify the effect on privacy rights.

Conclusion

36. Public debate about data security and about the privacy implications of governments' use of data mining for counter-terrorism efforts is important. Commissioner Thomas's report and these hearings are valuable parts of that debate. Thank you for the opportunity to contribute.

June 2007

APPENDIX 41

Memorandum submitted by Tesco

1. About Tesco

1.1 Tesco is one of the world's leading international retailers, employing over 450,000 people around the world. Our aim is to deliver a consistently strong customer offer on every visit and every transaction, in order to create value for customers to earn their lifetime loyalty.

1.2 We achieve this aim through two Tesco values; no one tries harder for customers, and treat people how we like to be treated.

1.3 Our customers have told us that trust is important to them; they trust us because they understand our values. In order to maintain this trust, it is important to ensure we are as open as possible. We try to apply the same principles of openness and honesty to our relations with all our stakeholders.

1.4 In order for Clubcard to be popular with customers and useful to us, it is paramount to maintain trust at all stages. Therefore, there is a strong commercial incentive for us to ensure that the privacy of our customer information is maintained at all times.

2. Understanding Clubcard

2.1 Tesco Clubcard enables us to thank our customers for shopping with us. It is a world-leading loyalty programme which allows us to better understand what our customers want and is an integral part of how we run our business as it helps us to listen to our customers and try and respond to their changing needs. Customers can collect an application form in-store, and register by freepost, by telephone or online.

2.2 Analysis of all Tesco Clubcard data is managed by Dunnhumby, a specialised provider of database management and analytical services. Tesco is the majority shareholder in Dunnhumby and controls all Clubcard data held by them. All personal information received by Dunnhumby is kept in a secure manner and processed in accordance with the laws relating to data protection.

2.3 In its role as our "data agency", Dunnhumby manage our requests for Clubcard data. This enables them to provide us with information on customer groupings for a specific campaign or project as well as enabling us to collate information in a manner that enhances our understanding of customer behaviour by segmentation or spend levels.

2.4 At no stage do we ask Dunnhumby to analyse information on individuals. This information is only accessed at the request of the Home Office or the individual customer.

2.5 Tesco is extremely proud of its Clubcard loyalty scheme, which rewards customers for continuing to shop with us. It enables consumers to get more from their shopping experience at Tesco by providing points that can be redeemed in-store or with a number of our partners.

2.6 The Clubcard scheme also enables us to utilise customer information to understand customer habits and improve the service that we can offer.

2.7 Every time that a Clubcard holder makes a purchase of over £1 in a Tesco store, online at Tesco.com, or on Tesco petrol, they can receive points on their purchase. In addition, points can also be collected by paying with a Tesco credit card, or paying for a Tesco mobile phone, a Tesco home phone, Tesco broadband at Tesco.net, on selected Tesco Personal Finance products and through Clubcard issuing partners such as Powergen and Avis.

2.8 For every £1 that is spent, customers usually receive one point. In certain circumstances, such as when allocating "green" points, we award two points for every £1 spent, and we also offer triple promotions on specific products.

2.9 At the end of every quarter, a Clubcard statement is sent out to all customers providing them vouchers reflective of the number of points they have collected and for other Tesco offers. One point is worth one penny, and vouchers will be sent out to all people that have collected over 150 points.

2.10 Points redeemed in-store are worth their cash value, meaning that £2.50 worth of points can be redeemed for £2.50 in money-off vouchers for Tesco stores.

2.11 Alternatively, Clubcard points can be redeemed against a range of products offered by our partners. Through our partners Clubcard points can be worth four times their in-store value. Our most popular deals are days out at attractions such as Alton Towers and Legoland, and we are now partnering up with theme parks in France and Germany.

2.12 Each Clubcard has its own unique 12 digit alphanumeric code to enable customers to log-in online where they can access their information and special offers.

2.13 Clubcard members are also able to join any of our clubs for free, including the Food Club, the Wine Club, the Baby and Toddler Club, and the Healthy Living Club. Members of these clubs receive a complimentary magazine relating to their chosen club, and a range of other benefits including money off vouchers and, in the case of the Baby and Toddler Club members, a free permit to park nearer to the front of the store.

2.14 In February 2007, we launched a partnership with the Open University so customers can now use their Clubcard vouchers to fund their learning, from a beginners course in writing family history to a humanities degree.

2.15 Last year nearly one million new customers signed up to Tesco Clubcard, and we gave away over £340 million in Clubcard vouchers to thank our customers for shopping with us.

3. Green Clubcard

3.1 We have recently begun to use Clubcard as a tool to encourage and reward green behaviour.

3.2 In August 2006, Tesco became the first supermarket in the UK to financially reward people for not using carrier bags. This means that customers receive a point for every Tesco bag that they do not use—and we do not restrict them to re-using our bags; shoppers can bring along carrier bags from any other retailer and still receive their points reward.

3.3 When Clubcard customers receive the quarterly statement, their total points tally includes a separate column dedicated to the number of "green" points collected. These are redeemable in exactly the same way as all other Clubcard points.

3.4 So far the bag reuse scheme has helped us save over 500 million carrier bags over the last six months.

3.5 Following the success of green Clubcard points in reducing carrier bag use, we have also tried to use it in other areas. For an eight week period, starting on 15 February, we gave away double green Clubcard points on products in our green and organic ranges, such as organic fruit and vegetables, energy efficient light bulbs and environment-friendly brands like Tesco Naturally and Ecover.

3.6 We also now offer Clubcard customers the chance to earn up to 500 points by recycling old mobile phones and printer ink cartridges. In return for recycling a mobile phone that will turn on, Clubcard customers will receive 500 green Clubcard points, or can choose for Tesco to donate £5 to the British Red Cross. For a mobile phone that does not turn on, or for a recycled ink cartridge, customers can receive 100 points or a £1 donation to the British Red Cross.

4. Customer Charter

4.1 Tesco recognises the importance of customer privacy and as such has created the "Customer Charter" to explain exactly what we do with stored information.

4.2 Personal details held by Tesco are never released to organisations outside of Tesco for their marketing purposes.

4.3 Customer details are used to send offers and discounts on products that we believe may be of interest to them. For instance, should a customer choose to tell us that they are a vegetarian, we will ensure that they only receive offers for non-meat products.

4.4 For those customers who tell us that they would rather not receive offers and other information, we only send a Clubcard statement every quarter. In addition, if a customer chooses not to be contacted for research, we promise them that they will not be bothered by us.

4.5 Should any customer wish to stop receiving our mailings and offers, all they have to do is to contact us to inform us of their decision.

5. Data Protection

5.1 Tesco has a clear "Data Protection Statement" in order to inform Clubcard customers of what we wish to use their information for.

5.2 This statement outlines our desire to utilise customer information to improve the Clubcard system and to understand customer habits in order to improve the service that we can offer.

5.3 At the point of sign up, customers choose from clear marketing options on the application form. Tesco does not contact those people who choose to opt out of receiving correspondence from us. Customers choose separately whether or not they wish to receive Tesco marketing material, third party marketing material and market research. All customers receive a quarterly points statement.

5.4 We comply with the terms of the Data Protection Act (1998) and all other relevant legislation and guidelines.

June 2007

APPENDIX 42

Memorandum submitted by J Trevor Hughes, International Association of Privacy Professionals

Executive Summary

1. The profession of privacy—meaning individuals skilled in counseling and managing the myriad issues related to privacy compliance and data protection—has grown significantly in the past ten years. The public and private sectors have now recognized that privacy professionals must be engaged in any discussion of new privacy standards, any development of privacy-sensitive technologies, or any initiative in which personal data is involved. Privacy professionals, in a very real way, bring to life the privacy protections promulgated by legislative and regulatory bodies around the world.

2. Enabling and empowering privacy professionals within the public and private sectors are effective ways to ensure that existing and emerging data protection standards are met. The opposite is also true: creating data protection standards without concurrently promoting the development of the privacy profession will undoubtedly ensure that standards are not met—and that the expectations of citizens with regards to the use of personal data are unfulfilled.

3. Privacy professionals have developed sophisticated tool kits to accomplish their jobs. Privacy impact assessments (PIAs) are one such tool. However, the profession of privacy has developed many other tools to respond to the challenges of maintaining trust and compliance in the information economy, including: privacy-sensitive product development, auditing, and privacy-enhancing technologies.

The Profession of Privacy

4. On behalf of the International Association of Privacy Professionals (IAPP), I am happy to provide these comments to the Home Affairs Committee's inquiry into the recent report commissioned by the Information Commissioner's Office, "*A Surveillance Society*?" The IAPP is a rapidly growing professional association that represents individual members working in the field of privacy and data protection. The organization works to define and promote this nascent profession through education, networking, and certification.

5. The IAPP currently has approximately 4,000 members in 23 countries around the world. We are based in the United States, however a sizable number of our members come from the UK and, more broadly, the European Union. One of our largest and most active chapters is located in London—with members gathering regularly to discuss issues related to the regulatory and operational challenges in today's information economy.

6. It is important to note that the IAPP is not an advocacy organization, and does not take policy positions on substantive matters related to data protection. We endeavour to provide our members with a great breadth of educational offerings in the field of privacy, but we do not take any position on the merits or faults of particular privacy laws, regulations, or programs.

7. There is one large exception to our rule against taking advocacy positions: we feel strongly that privacy professionals are a critical component to any of the responses to privacy concerns in the public or private sectors. Put simply, you cannot have effective privacy practices without skilled practitioners to define, create and maintain them. We feel that any discussion of appropriate responses to data protection challenges must necessarily include recognition of the need for privacy professionals.

8. The IAPP was founded six short years ago when an emerging network of privacy professionals recognized the need for a professional association. The organization has grown rapidly since those early days and now boasts over 4,000 members in 23 countries. Our recent annual conference here in Washington was, to our knowledge, one of the largest privacy conferences ever held, with over 1200 attendees. Clearly, the market has placed a very high value on privacy and the robust, but responsible use of data.

9. When the IAPP was initially formed, the majority of our members shared a similar title: chief privacy officer, or CPO. Indeed, many—if not most—multinational companies have now appointed a chief privacy officer. But the majority of IAPP members are not CPOs. Rather, we have seen a robust hierarchy of professional roles in privacy emerge. These privacy professionals cover issues of compliance, product development, marketing, security, human resources, customer relations, and more. The management of privacy issues in large organizations now requires a broad and deep team of professionals with increasingly sophisticated skills.

10. It should also be noted that the United States, while not having a privacy commissioner, has required all federal agencies to appoint a representative to be responsible for privacy issues within that agency. Through this requirement, many governmental chief privacy officers have been appointed. Further, we are beginning to see the appointment of chief privacy officers at the state level—with California and Ohio both having privacy functions created within state government. These federal and state privacy professionals have a distinctly different function than, for example, the UK Information Commissioner. Governmental privacy professionals in the United States are not regulators. Rather, they are responsible for overseeing and, in some cases, managing an agency's use of data.

11. The job of a privacy professional demands mastery of a complex set of laws, technology, security standards, and program management techniques. Many privacy professionals are also legal professionals, but other fields—such as accounting, technology, marketing, and security—are well represented within our membership.

12. In 2004, the IAPP introduced the first broad-based privacy certification to the US marketplace, the Certified Information Privacy Professional (CIPP). This credential is meant to serve as a demonstration of a candidate's mastery over a range fundamental privacy concepts. The CIPP program covers: law and policy; online privacy; information security; operations (managing a privacy program); and data transfers. To date, roughly 2000 people have taken the exam and over 1500 CIPPs have been granted worldwide. We feel strongly that the CIPP program is a crucial component to the continued professionalization of this field.

13. In 2005, the IAPP extended the CIPP program to include issues of governmental privacy. The CIPP/G program covers issues specific to the US public sector: such as the Privacy Act, the eGovernment Act, the Patriot Act, and more. Included in this designation is a significant focus on privacy impact assessments (PIAs), which are required of many government programs in the United States under the eGovernment Act.

Privacy Impact Assessments

14. Again, the IAPP does not take a position on whether a legislative requirement such as the PIA is good or bad. However, I can say that PIAs have become a very commonly used tool for privacy professionals to assess the potential data protection implications of a program prior to launch. Our members actively use such tools on a daily basis. In general, it appears that PIAs have provided an important mechanism for privacy professionals to assess and provide commentary on new programs within federal agencies.

15. Generally, the Department of Homeland Security describes a PIA as an analysis of how personal information is collected, used, disseminated and maintained by a US federal agency. The PIA examines how the agency has incorporated privacy concerns throughout the development, design and deployment of a program or technology.

16. A recent assessment by the US Office of Management and Budget (an oversight body for US governmental agency operations) found that the US Department of Homeland Security (DHS) conducted 25 assessments in 2006, up from only 11 such assessments in 2004. However, this was against a backlog of 143 DHS programs which required PIAs in 2006. In total, the DHS has completed 70 PIAs since the inception of the eGovernment Act requirements.

17. Commentators have applauded PIAs as a good mechanism for providing substantive feedback on the development of new programs. Further, the transparency afforded to citizens as to the uses of their data by the government can only be seen as a positive factor.

Other Tools Used by Privacy Professionals

18. There are other tools used by privacy professionals to effectively manage privacy within an organization. Certainly, PIAs are one such tool. However, PIAs should not represent an assessment of data protection issues *after* a program or technology has been conceptualized. Many privacy professionals, particularly in the private sector, are actively involved in the actual development of products and services for their organization. This is particularly true in the technology industry. Indeed, the assessment of privacy concerns often occurs during the *development* of a product or service—as opposed to after, when the product

or service may be ready for release to the marketplace. Organizations that engage in this type of privacy-sensitive development may find that there are fewer delays and smoother paths forward for the release of new offerings. Ideally, PIAs should be seen as an iterative process—one that involves an ongoing involvement by privacy professionals through the design, development and deployment stages.

19. Privacy professionals also actively manage audit and accountability programs to ensure that any privacy protections built into programs are actually working in the manner intended. We have certainly found that privacy issues cannot be managed effectively from a distance. Privacy professionals must become actively involved in overseeing the use of data (through audits and other controls) to ensure that expectations regarding privacy are indeed met. In fact, a substantial industry of external privacy auditors has emerged around the world to help to review and assess compliance with both privacy laws and internal privacy policies.

20. We have also witnessed the development of privacy enhancing technologies in the marketplace (PETs). Some PETs are available to the marketplace as responses to concerns associated with disruptive or troubling privacy practices. Anti-spyware programs, spam filters, and pop-up blockers are good examples of such "after-market" solutions. Other PETs are built into the technology itself. Within many internet browsers, controls exist to manage and block privacy-sensitive technologies such as cookies. Indeed, Microsoft's Internet Explorer browser includes a sophisticated tool which requires certain cookies to be associated with a condensed privacy statement. Failure to associate some cookies with a privacy policy may result in them being blocked outright by the browser.

21. It must be said again that any of the tools described above are useless without trained and skilled professionals to use them effectively. My personal experience is that the addition of privacy professional to an organization's staff can only improve that organization's respect for personal information. Privacy professionals are, quite simply, good for privacy.

Conclusion

22. Clearly, the profession of privacy has cemented its position as a critical resource in any organization that deals with data—whether in the public or private sectors, or both. I encourage members of the committee to visit the IAPP's website, www.privacyassociation.org, to learn more about the profession of privacy. And, as a CIPP myself, I strongly recommend that the committee consider the value of such privacy certifications as a tool to ensure privacy issues are properly identified and addressed in the public and private sectors. I thank you for this opportunity to testify before your Committee today.

June 2007

APPENDIX 43

Memorandum submitted by Dr Ian Forbes

This submission is intended to complement the evidence submitted to the Committee by the Royal Academy of Engineering. Dr Ian Forbes was a member of the Royal Academy's Working Party on Privacy and Surveillance, and contributor to the Academy's Report, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. His submission includes additional reflections, in response to the specific concerns of the Committee's Inquiry.

Principles and Themes

The organising principle of the Report of the Royal Academy of Engineering is that protecting privacy, achieving greater levels of security and maximising utility will always generate dilemmas for individuals, government 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 successful. The costs of not recognizing and addressing these dilemmas include a decline of public trust, inefficient allocation of resources, and avoidable failures.

Upstream Actions

- The design of any system that collects and processes personal data must have a primary focus on privacy.
- IT projects that include the collection and processing of large amounts of data must have thorough risk assessment procedures and effective implementation mechanisms.
- Accepting that failures will occur, incorporate appropriate procedures.
- Make reciprocity a design feature.

Principles in Practice

- People occupy many roles, so it should always be possible for an individual to keep these roles separate, and to preserve the distinction between identification and authentication.
- Data sharing should only carried out when there is an explicit need and reason.
- Personal data should only be used for the purposes for which consent has been given.
- In general, public agencies should not be allowed access to private databases.
- Public record databases should be under the control of autonomous agencies, not government.
- Penalties for misuse and abuse of personal data should reflect the damage and distress that the system failure or crime causes.

CCTV, Social Goods and the Citizen

New and emerging technologies which explore and exploit the capacity to collect, store and manipulate data about citizens and their behaviour are much deployed by industry and the police and security services. Much of the debate, and much policy, focuses on the security aspects of the way that organisations use these technologies for profit and convenience. In relation to crime and security, the emphasis is almost entirely on public safety.

This is especially true for surveillance technologies involving cameras. There are serious concerns about the proliferation of this technology, and the quickly-evolving capacity digitally to store, interpret and transmit human images. At present, these technologies are largely restricted to users who want to prevent, monitor and sometimes punish certain behaviours, despite the lack of evidence that surveillance alone is effective. Apart from the problems associated with general invasions of privacy, specific problems of predictive profiling of some sectors of the community arises with the increased capacity to identify individuals, and target apparently "deviant" or "unusual" behaviour. The design assumptions that are built into these technologies are as important as the assumptions of the human operators of these systems. Failures in any of these systems expose the fragility of public trust, and can contribute to a lack of trust not just in the systems, but government and its agencies.

Hardly any attention has been paid to the positive uses of this technology. Communities have long had a justifiable interest in their public spaces, in who uses them and how. However, local communities and citizens under surveillance have few if any opportunities to see and learn from what the vast number of cameras see. The uses and benefits of this technology are currently under the control of the operators, who effectively own the images and data of citizens without having gained their consent. Unless and until ordinary citizens are given an active stake and a determining say in the processes and practices of camera surveillance, new and socially beneficial uses of these surveillance technologies will emerge only very slowly, or not at all. A new approach is needed, which introduces a climate of candour and a requirement of reciprocity, so facilitating creative input from communities and citizens. Finally, creating opportunities for citizens to contribute to the design and use of these systems will help broaden the basis for trust.

Recommendations

- The right to conduct surveillance should generate reciprocal rights for those under surveillance.
- Purposes, placement, conditions of use operating practices and personnel should, by law, be subject to consultation, agreement and challenge by those under surveillance.

Public Policies and Privacy

The full range of policy tools should be employed:

- improve privacy law;
- initiate new legislation to set high design standards, require best practice implementation and make compensation for system failures routine and costly to operators—in other words construct an effective incentive structure;
- increase the powers for the IC, including audit power and greater penalties;
- establish a new body to oversee the collection, retention and use of bioinformation (including DNA profiles, fingerprints, facial images and so on);
- encourage and reward industry initiatives;
- government and its agencies need to set the highest standards;
- introduce reciprocal rights for those who supply personal data in any form;
- facilitate debate on privacy and security dilemmas; and
- inform and consult widely on policy options.

The Case of Privacy Impact Statements

PIAs are not a proven mechanism for producing effective change or reliable information.

They may have the unintended consequence of diverting energies into a new bureaucratic procedure—and a new wave of consultants—that fails to lead to productive change. (The experience of EIS is instructive.) PIAs, in other words, could work against privacy.

Many PIAs would quickly gravitate toward being a standard, defensive document, containing:

- Predominantly obvious conclusions, with similar findings reproduced in almost all PIAs.
- Disclaimers about important aspects of privacy impact which are characterised by uncertainty.
- An assessment that will never identify an unintended and unforeseeable consequence.
- Assumptions that all other things remain constant. Changes of circumstance, technology, legislation and practice could vitiate any PIA at any point after its completion.

Recommendation

Monitor the introduction of PIAs in Canada in order to assess their efficiency in protecting privacy, their bureaucratic efficacy and opportunity costs.

Information on Databases

Recommendations

- Personal data should never be scored in unencrypted form.
- The minimum amount of data should be kept for the minimum amount of time.
- Personal data in large databases should be checked regularly with data subjects to ensure that they are accurate.
- If a database contains personal data about many people, or vulnerable people, the database access software should be developed to very high standards of security engineering.
- If data are lost, individuals affected must be informed and compensated swiftly.
- Systems should be designed to keep an automatic audit of when the data are accessed and by whom and especially when data are changed.
- Profile-based decision systems should be open, accountable, contestable and non-discriminatory.
- The national DNA database should be used only to store the DNA profiles of those individuals involved in criminal proceedings.

June 2007

APPENDIX 44

Supplementary memorandum submitted by the Loyalty Management Group

We refer to the Evidence heard in public by the above Committee on 7 June 2007 and, in particular, the Chairman's comment in Q161 (page 45) of the uncorrected transcript of oral evidence.

The Chairman has requested further information on how loyalty card data is used and whether the customer has any control over it in the context of the preceding questions relating to use for supermarkets' strategic planning purposes.

As explained in our oral evidence, Nectar does not use data for strategic planning purposes for Sainsbury's (as the company issuing Nectar points in the supermarket sector) and, under Nectar's Policy on Privacy and Data Protection, information provided to Nectar is to be used for marketing purposes. Sainsbury's, of course, also obtains information itself when consumers buy products in its shops and, as we also explained in our oral evidence, can access data held by Nectar on Sainsbury's customers.

As to whether consumers can control the use of their data for such purposes, participation by consumers in Nectar is entirely voluntary and the purposes for which their data will be used is clearly disclosed to consumers before they join the programme as part of the registration process. Consumers are able to opt out of the purposes for which Nectar holds data at any time, whether in writing, over the phone or by using the My Account facility on the Nectar website. However, as these purposes do not include strategic planning purposes, such an opt out is irrelevant and so does not appear.

As noted above, Sainsbury's does have access to Nectar customer records to the extent that they are Sainsbury's customers but only Sainsbury's customers. We would expect that Sainsbury's, like many other businesses, would use all the resources and information at its disposal in making important decisions, including quite possibly the location of its shops. We believe that consumers would be aware that Sainsbury's might use the information it has available on its customers' shopping behaviour, as well as other information available to it, for any legitimate purpose. Such other information in this context might also include, amongst other sources, electoral roll data, generally available lifestyle data (e.g. Acorn), market research data and demographic studies.

The specific point made by the Chairman at the hearing on 7 June was whether shopping patterns could be used to have a district shopping centre put out of business by a new superstore. With respect, we consider that such matters are of limited relevance to the issue of "A Surveillance Society?" and are already governed by other legislation (e.g. planning legislation, competition law) and other enquiries, such as the current market investigation into the supply of groceries by supermarkets being undertaken by the Competition Commission after referral by the Office of Fair Trading in May 2006.

June 2007

APPENDIX 45

Supplementary memorandum submitted by Dr C N M Pounder

At the end of the oral evidence (26 June), the questioning turned to what could be done to improve the supervision of surveillance. As we had run out of time, I thought it useful to produce a list of improvements that are, in my view, essential to help maintain public trust if surveillance is to occur.

10 Standards of Trust to Safeguard the Individual

It is my belief that safeguards have to meet 10 "standards of trust" that demonstrate to the public that their privacy interests are safeguarded and that they can trust the *complete process*: from law-making to dealing with law-breaking. It will be useful to identify these standards so that any Bill of Rights can accommodate them. They apply to any activity which involves the processing of personal data, surveillance or interference by a public body and the standards can be listed as:

1. Any processing/surveillance/interference is limited to lawful purposes approved by Parliament.
2. Widely drafted powers or laws are not used to legitimise extensive function creep without detailed scrutiny by Parliament.
3. Procedures which authorise processing/surveillance/interference are followed scrupulously.
4. Procedures which authorise processing/surveillance/interference are separate from procedures related to the doing of the processing/surveillance/interference itself.
5. A complete record of the processing/surveillance/interference and its authorisation is retained to ensure transparency and accountability to the system of supervision.
6. Staff involved in the processing/surveillance/interference activity are fully trained to follow the rules.
7. Any malfeasance can be identified and individuals concerned suitably punished.
8. The system of supervision is independent of Government, well financed, and has effective powers of investigation and can delve into operational matters.
9. The regulator in charge of the supervision reports to Parliament and can refer matters to Parliament.
10. Full compensation for aggrieved individuals when things have clearly gone awry.

The thrust of my other written evidence was that reliance on data protection and human rights law is insufficient. However, meeting these trust standards in turn requires changes to Parliamentary procedure, to the Commissioner's powers and to the individual's level of protection. These additional safeguards are outlined below.

Safeguards Involving Parliamentary Procedure

Parliament has traditionally balanced the public interest by scrutinising the executive. To assist this:

- Parliament should have a mechanism which allows it to demand any information that relates to the processing of personal data/surveillance/interference (eg publication of details or legal advice that explains why there is no breach of the Article 8; why the European Commission considers the UK's Data Protection Act to be defective and why the UK Government says it is not).
- Parliament should become involved in the details of the processing of personal data/surveillance/interference when matters are referred to it. For example, there are several Codes of Practice (or parts of Codes) that concern these issues that the Secretary of State currently lays before

Parliament. These could be subject to consultation with a Commissioner. If consultation results in agreement the Code can come into effect without Parliamentary involvement. If agreement is not forthcoming, Parliament should have to approve the Secretary of State's Code by positive affirmation. This means that Parliament can explore the reasons for the disagreement.

— Parliament should separate privacy and security responsibilities. All warrants that concern surveillance or interference, currently signed by a Secretary of State, should seek judicial approval. This step would automatically separate the power to authorise interference from the mechanisms that protect an individual from unnecessary interference.

— Parliament should permit a Select Committee to take privacy under its remit. Currently such issues have only been discussed in the narrow context of a Committee's specialist remit (e.g. child protection and privacy, science and privacy in relation to the DNA database; Home Affairs and privacy, etc) with the result that the big picture of how *all* Government initiatives impact on privacy has yet to be reviewed.

— Select Committees of Parliament should allow, if they decide, experts in the field to ask questions. In cases which relate to the scrutiny of public policy towards privacy, often the devil is in the complex detail of *how* surveillance occurs and not on the broad principle of *whether* surveillance should occur.

— Parliament should insist that the various Commissioners who have a role to ensure that any surveillance/interference is proportionate should report to Parliament and not to the Government Minister that is responsible for the interference. The Commissioners should also be able to employ security cleared experts to investigate operational matters where this is needed and a single Commissioner should deal with all national security issues.

Safeguards Involving the Powers of a Commissioner

— A Commissioner should be able to insert into any relevant Code of Practice that relates to an activity concerning the processing of personal data or surveillance or interference:

  (a) any procedure that establishes proportionality before any activity is commenced;

  (b) the criteria which measures the success of the activity; the compilation of records that show that the activity was properly authorised including the statistical data which can used to demonstrate transparency or that the interference was justifiable in terms of outcomes from performing the activity; or

  (c) require a Privacy Impact Assessment or audit to be undertaken.

— A Commissioner should be able to test Article 8 in the Courts (eg he could be provided an "Article 8 (Incompatibility) Notice" which can test whether a particular Statutory Instrument or primary legislation is compatible with Article 8 of the Human Rights Act.

— A Commissioner should have effective powers of investigation, intervention, audit and prosecution that can extend into operational matters.

— A Commissioner should have the duty to ask for changes to Codes of Practice or Ministerial powers that, in his view, would rectify a pressing privacy problem. Such a mechanism could provide, in cases where the Minister disputed the Commissioner's view for Parliament to refresh its approval of Ministerial powers or Code of Practice by an affirmative Statutory Instrument procedure.

Safeguards Improving the Individual's Level of Protection

— Individuals should be granted a right to privacy of personal data, via the Sixth Data Protection Principle, which can be enforced by the Information Commissioner.

— Individuals should be informed when their personal data have been lost by an organisation in circumstances where the data could be used for ID theft. This obligation could arise by the introduction of a variety of USA security breach legislation where individuals are informed when unencrypted personal data are lost. Alternatively the legislation could specify that when a certain kind of security breach arises, the organisation has to notify the Commissioner of a security breach, and then the Commissioner decides whether individuals should be notified that their personal data have been compromised.

July 2007

APPENDIX 46

Memorandum submitted by the Department for Children, Schools and Families

DATA GATHERING AND DATA SHARING WITHIN THE DEPARTMENT

Introduction

1. Effective sharing of data and information is central to the Department for Children, Schools and Families (DCFS) 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. While better information sharing brings many benefits, the Department 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.

The Benefits of Data Sharing

3. Much of DCFS 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 DCFS, 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 and skills 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. DCFS has many major programmes that depend on effective sharing of data. While all 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 DCFS and DH sharing the policy lead for children and for vulnerable adults respectively. Other DCFS programmes are about enabling efficiency, and improving educational attainment. For example, 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.

5. We are currently working with a group of Local Authorities piloting Electronic Common Assessment Framework systems (e-CAF systems). They are ensuring access is controlled by one individual in the Local Authority. This work is at an early stage and we are already working with the Information Commissioner to ensure we take his views into account.

6. 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.

7. 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.

8. 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.

9. 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.

10. The New Deal for Skills (NDfS) programme is currently at pilot stage but also demonstrates some of the advantages that come to both citizens and society at large from effective data sharing, NDfS provides tailored support to help unemployed people develop the skills necessary to sustain and progress in employment by enabling those with low skills or a lack of qualifications to access training provided by the Learning and Skills Council. NDfS also helps to ensure that the training provided is appropriately targeted at those who need it by evaluating the effect of training on job retention and career prospects. Information is shared in two key ways. Firstly, information about unemployed people and their skills is shared between advisers to help them identify suitable training. Secondly, information is shared to evaluate the programmes and see how effective it has been in terms of helping people into work. Data sharing also benefits the taxpayer and wider society by ensuring that benefit claimants attend their specified training courses, increase their skills, come off benefits and enter the workforce. Responsibility for the NDfS programme has been transferred to the Department for Innovation, Universities and Skills following the recent Machinery of Government changes.

11. In contrast to NDfS, 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.

Privacy and Security of Data

12. While these examples demonstrate some of the benefits of data sharing to both the citizen and administrative systems, the DCFS 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.

13. 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.

14. Additionally 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 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 guidance advises School governing bodies and head teachers (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.

15. 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 theats, 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.

16. Data security is being built into the design and implementation of all the major DCFS 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.

17. 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 ContactPoint operators 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 for more details of ContactPoint

18. 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. 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.

Vetting and Barring Scheme

19. As a final example 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.

20. 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).

In Conclusion

21. The Department takes very seriously issues around security and confidentiality of data to ensure that it is only used for purposes for which it is intended. In particular 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.

July 2007

Annex

ContactPoint

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.

ContactPoint is being established under section 12 of the Children Act 2004. Draft regulations made under this section are currently being finalised and are due to be laid before parliament before the summer recess. These regulations are subject to affirmative resolution.

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.

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.

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 co-ordinated support.

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 is made clear in the draft ContactPoint guidance, currently available for public consultation (closes 27 July 2007).

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.

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.

The draft 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.

July 2007

APPENDIX 47

Memorandum submitted by Dr Andy Phippen,[238] Dr Hazel Lacohee,[239] and Professor Steven Furnell[240]

In this response to the call for evidence for the Home Affairs Committee's inquiry into "A Surveillance Society", we present a response that considers the citizen's perspective, examining their perceptions toward monitoring via various ICTs, before considering their awareness of protection mechanisms. The evidence presented is drawn from a major study in collaboration with BT Group Chief Technology Office and Hewlett Packard, supported by a number of further studies carried out by the University of Plymouth's Information Security and Network Research Group.[241]

The Trustguide project[242] was concerned with exploring issues of trust, security and privacy in ICT based applications and services with the general public through direct dialogue, facilitated via 29 discussion groups between September 2005 and October 2006. In total approximately 400 citizens took part in discussions. 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. This has significant implications for service providers and policy makers—the age of the naïve ICT user is over, replaced by a population who may not have experienced specific technologies first hand, but have confidence in their understanding based upon numerous information sources (albeit from sources that one might consider to be unreliable or subjective sources). We are faced with a population who believed they are well-informed regarding their understanding of ICTs, and are cynical when "sold" a technology for reasons that conflict with their own belief systems.

In considering surveillance technologies, and citizen's attitude toward such, one of our more interesting initial findings was the tolerance of UK citizens toward CCTV monitoring. We felt, through our initial discussion, that citizens would be intolerant of such systems. However, in-depth discussion provides two key reasons why such tolerance exists. Firstly, CCTV exists in public spaces—people do not mind monitoring

[238] Information Security and Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Drake Circus, Plymouth, UK.

[239] BT Group Chief Technology Office, Adastral Park, Martlesham Heath, Ipswich, UK.

[240] Information Security and Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Drake Circus, Plymouth, UK.

[241] http://www.network-research-group.org/

[242] http://www.trustguide.org.uk/

when it is open and not invasive of their private space (their homes, workplace, etc). In addition, media coverage of crime and terrorist attacks had demonstrated the value of CCTV in protecting society. The power of the media as a persuasive mechanism for the general public should not be underestimated, and it is something that we will return to later in this piece.

However, this attitude should not lead to Government complacency related to further monitoring. 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. 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.

We have found this opinion results from a number of different beliefs. Firstly, as we have stated above, CCTV is tolerated because its benefits are clear to see via the media. Technologies such as ID cards, biometrics and DNA databases have less of an "evidence base" from which citizens can draw to inform their opinions. An important key finding from our work is that technological engagement with the general public has little to do with technical elegance, guarantees of security, and reliability. It does, however, have a lot to do with convenience for the citizen. If the citizen can see a clear benefit for either themselves or their community (whether their concept of community might be) they will be far more accepting of a technology than one where they cannot see such.

So if we consider the issue of ID cards, we can see difficulties in being able to demonstrate the benefit to the individual. Indeed, what is the benefit for the individual in carrying an ID card? Clearly there are benefits for Government, security services and industry, but the individual can see little benefit to having one in their possession. Therefore, with an unreliable foundation upon which to build trust in ID cards, there is little wonder that further opposition is met with the proposals to have mandatory ID cards paid for by the citizen.

Another key factor in the public's mistrust of surveillance systems is again something drawn from media influence. Numerous participants in our discussions stated that the Government were not effective at "doing IT". High profile public sector failures, or predicted failures, such as the Child Support Agency system, have resulted in a public who do not feel that the Government are capable of effectively managing the systems required to ensure the efficient operation of such surveillance system. Therefore, guarantees of 100% secure 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. Compounded with this mismanagement is another factor that has eroded the public's trust of the Government looking after "their" data (individuals clearly believe that data held about them still belongs to them). There were subsections within many groups that were uncomfortable, not from the privacy issues but because they felt if the Government had physical ownership of that data, there might be temptations to sell such information to interested bodies, as has occurred with DVLA data.

We believe that the Government's key issue with the acceptance of a reasonable "Surveillance Society" is not one of technology but education and informing the population. We have discussed at length the information sources that citizens draw upon when forming opinions regarding ICT—the main influencers are the media and peers. While those citizens that have access to professional advice will take it, the majority of their awareness comes from what they see in the newspapers, what they watch on television, and what they discuss with their peers.

A key issue Government faces is that these information sources do not have an objective viewpoint. Arguably, the World Wide Web is a major threat to the media industry—therefore, where is the incentive for a media outlet to report "citizen uses ICT successfully to enrich life"? Previous attempts to use the media to disseminate objective material about Internet awareness and protection have only had limited impact. We discussed the Get Safe Online campaign[243] within both the Trustguide and subsequent survey work (surveying approximately 500 citizens regarding their ICT security practices and their sources of education), and in each case, impact had been minimal. In the survey responses, 12% of the population was aware of the campaign and only a third of those felt the information was useful.

However, there is a belief among citizens that, while they have opinions regarding ICT and its threats, they do not have the confidence or concrete knowledge to protect themselves. In our survey work, the majority of respondents felt that they did not do enough to protect themselves from online threats for a variety of reasons, including lack of understanding, cost of products, or that they simply did not feel it was their responsibility. This was reflected in our Trustguide discussions, where many participants stated that either they did not feel equipped to protect themselves, or it was someone else's job to do so. When discussed in more detail, the responsibility for protection, in the eyes of the citizen, normally lies with either Government or manufacturers and service providers. There were many comparisons with motor vehicle safety, where citizens would not expect to purchase a car without it being roadworthy.

[243] http://www.getsafeonline.org/

However, some of our recent research would suggest that while IT providers are doing more, citizens are still failing to take any responsibility for protection. In carrying out a survey of unprotected wireless network access in cities and towns in the South West, we discovered on average around 25% of networks were not encrypted. This is a significant change from previous years, where generally around 60% were found to be unprotected. This change corresponds with a period in which the wireless hardware provided by vendors is now encrypted "out of the box". This means that the individual does not have to set up the encryption themselves, it is there by default. This represents a significant shift for IT vendors in taking steps to protect the citizen.

Around the same time, a complementary experiment scanned for unsecured Bluetooth devices and, when discovered, the devices were sent a harmless, but unsolicited, image file. In over 50% of cases, the recipient was happy accepted the file without querying what it was or where it came from.

These experiments show that while manufacturers taking greater responsibility to protect the public, some of the responsibility ultimately has to rest with the citizen. To take the motor vehicle analogy once more, someone purchasing a car and driving it home is not faced with an ever-evolving environment with new threats emerging on an hourly basis. However, this is exactly the environment facing IT users. Therefore, we feel we should stress the importance of reaching the public with accurate, objective information regarding ICTs so they can make informed decisions, rather than the current climate of building belief systems on very weak, ill constructed, foundations.

Of more immediate concern is the protection of young people. Within our discussion with young people, it became very apparent that while they were technically capable, they had little awareness of the threats that exist in going online, and only had a veneer of knowledge regarding protection mechanisms. On three separate occasions in discussions with young people, we encountered experiences of stalking attempts via messenger services. While in all three cases, the perpetrator was blocked by the intended victim, there was no reporting of the incident to an authority figure. When asked why not, the responses ranged from "what's the point?" to "I didn't know how to". The majority of young people we spoke to felt that authority figures (such as parents and teachers) had less knowledge about online threats than they did, and as such would not know what to do either.

This discovery led to further investigation into the exposure young people get to Internet awareness and protection through school curricula. Certainly GCSE and A-level curricula for ICT and Computing that we examined had virtually no mention of protection mechanisms, aside from those to deal with business ICT. However, we found that young people are receptive to the idea of classes in such an area, some suggesting Citizenship classes could cover such things. Certainly, the work of the Child Exploitation and Online Protection Centre,[244] with their schools programmes, is having an effect, but this is a small Government department reaching out the approximately 25,000 schools in the UK. Young people also felt the media could play a part, but were more likely to be engaged through drama than direct information presentations.

In considering the safeguards for data use, and abuse, we finally consider legislative measures. While our studies with citizens have shown some awareness of measures such as the Data Protection Act and other legal mechanisms to ensure adequate protection, we also, unsurprisingly, discovered that the majority of citizens will not consider things such as Terms and Conditions in depth when registering with an online service, particularly if such a service is offering them some sort of material or social benefit. Obviously this can potentially leave the citizen open to all manner of data abuse, but the general opinions were that while they knew they should read such things, they lose interest in the legal syntax of such. Therefore, stronger legislation to ensure more effective privacy policies would have little impact.

However, we believe there is one area that could potentially have more significant impact is more effective regulation of the service providers. At present, there is little professional liability within the IT industry. Hence the number of breaches and information thefts that occur online, the majority of which are down to poor security practices, design and implementation, rather than issues with the technology itself. The IT industry is one driven by the sort of remunerative rewards that one might expect from any professional discipline, but without the legislative controls that apply to, for example, the legal or medical professions. Therefore, service providers are happy to commit to service delivery without actually considering the feasibility of such approaches. Certainly, our own experiences acting as intermediaries between clients and service providers when troubleshooting what went wrong in projects would suggest the lack of legislative control results in a highly unregulated industry without some extremely unethical practice. While the British Computer Society is making great strides forward with its professionalism agenda, its membership is still only a small part of the IT industry, and complimentary to their reward-based incentives to become an "IT professional" could be stronger legislation. A service provider may become far more likely to carry out effective risk analysis, and penetration and boundary testing, on their services if they were to be held accountable for any avoidable breaches, in the same way that society would expect a surgeon behaving in an unethical manner would be held to account. Currently, we exist in a culture of "well, you signed-off the specification" where the responsibility is placed back with the procurer, rather than provider, of a service.

[244] http://www.ceop.gov.uk/

In conclusion, we believe that while technology has a part to play in the public attitudes toward whether we exist in a "surveillance society", the major issue lies within the public perception of such approaches—whether they consider them to be acceptable and good for the private citizen. We believe education and information are key drivers in ensuring a society that is more aware, and accepting, of *realistic* surveillance measures in place to protect them. Our work also suggests that understanding of public perception still requires far more work, as our discoveries about the public's attitudes toward ICTs is in conflict with conventional wisdom. Finally, we believe that dividing responsibility between citizens and service providers is necessary to ensure more effective safeguards, and feel that stronger legislation of the ICT industry, with greater awareness of professional liability, is an important step forward in achieving such protection from data theft and abuse.

July 2007

APPENDIX 48

Supplementary memorandum submitted by Tesco

Thank you for the recent opportunity to give oral evidence on Tesco's behalf to the Home Affairs Select Committee inquiry on *A Surveillance Society?*

In response to Mr Denham's questions relating to the strategic use of Clubcard data, I would firstly like to challenge the suggestion that Clubcard is used to put local shops out of business. This is simply not true. The primary role of Clubcard is to enable us to thank our customers for shopping with us and enable us to better understand what they want and try and respond to their changing needs.

I understand Mr Denham's concerns about the future of local shopping centres but would like to emphasise that investment by Tesco can really benefit a local area. Not only do our stores bring improved choice and a greater range to customers, but the popularity of our stores can be a rejuvenating force in a local area, increasing footfall and custom for all local shops, and improving the vitality of the neighbourhood around the store. Academic studies have shown such positive effects in a number of areas where we have developed new stores, such as in Beverley, Glasgow, the Seacroft area of Leeds and in Hampshire. I would be more than happy to provide more detail on these studies should this be of interest.

To turn to the specific question of the use of Clubcard data, aggregated data can help us understand the demographics and trading patterns of a local area. This can in turn help inform our planning for new stores and enable us to offer customers the best possible new shopping environment. However, all analysis of Clubcard data for this purpose is based on aggregated and anonymised data and confined to spending patterns and postcode data, rather than individual customer information.

It is also worth making the point that whilst Clubcard data can be used to understand local demographics, this sort of information is also available through Experian or the National Survey of Local Shopping Patterns.

Finally, as I explained during the oral evidence session, we have worked with our customers to ensure our Clubcard application form gives them sufficient information about how we use their data and enables them to opt-out of marketing where they wish to, which customers have indicated is most important to them. We recognise how important privacy is to our customers and ensure that we comply with all relevant legislation and good practice guidelines in the way we process and use their personal information.

I hope that I have been able to address your concerns.

July 2007

APPENDIX 49

Memorandum submitted by Mr Malcolm Hurlston

Founder and Chairman of Consumer Credit Counselling Service (CCCS), Britain's largest debt-advice charity. It currently manages around a 10th of UK problem debt. CCCS maintains an industry leading database on people in debt.

Chairman of Registry Trust Ltd, a not-for-profit organisation which maintains the register of Judgments Orders and Fines on behalf of the Lord Chancellor. Chairman of Hurlstons, which devised the original principles of reciprocity for the sharing of data among lenders.

DATA

1. Most of these comments relate to the credit industry where I have a large amount of experience and knowledge.

2. Despite calls from the banking/credit industry for more data to be shared no amount of data sharing will help in at least half of the cases seen at CCCS. Debt is mainly caused by life problems.

3. Some banks currently do not share across their total portfolios, let alone among themselves. Recently merged banking groups can still operate as completely separate entities with little communication between them. If there were a convincing case for data sharing they would have taken speedy steps to share internally.

4. Previously my consultancy provided some of the expertise which came up with the principles of SCOR.[245] Representing SCOR I argued to the government at the time that the industry would not need more data in the future. Work on predictiveness would mean that inefficiencies could be avoided and that the data would in effect be better used than in the past.

5. In the United States data is routinely shared among lenders. The absence of a paper about this from the protagonists of data sharing in the UK indicates the case for its effectiveness in the world's largest credit market may be weak.

6. Data sharing is promoted by the credit industry more generally as the cure for over-indebtedness. However, as I have attempted to prove above, the case has not been made.

7. This paper is submitted in a personal capacity.

August 2007

APPENDIX 50

Memorandum submitted by Her Majesty's Government Chief Information Officer

1. INTRODUCTION

1.1 The Ministry of Justice (MoJ) is responsible for the Government's domestic policy on data protection and data sharing and represents the UK at European and international level.

1.2 This memorandum sets out to cover the roles of the CIO Council, Her Majesty's Government Chief Information Office and the Transformational Government Strategy.

1.3 It does not provide detail of specific examples of public and private databases in existence as this is the accountability of the Departments, who "own", collect or process this data.

1.4 The Transformational Government Strategy enabled by Information technology was approved by Ministers and published in November 2005. It set out three core themes. The first theme firmly positions the Citizen at the heart of the Public Services and ensures that products and services which are implemented meet the needs of the consumer not the product or service provider. The second theme sets out to ensure that the Public Sector moves to a shared culture—in the front office, the middle office and the back office. And finally the third theme focuses on the professionalism and capability of the Public Sector to deliver IT enabled business change.

1.5 The Transformational Government strategy is underpinned by 13 strands of work, several of which are relevant to this committee. They are:

1.5.1 Identity Management—Before you can share Citizen Data you must be sure that you have identified the correct Citizen before data is shared.

1.5.2 Data Sharing—How do we share data appropriately across the Public and Private sector to aid the efficiency and effectiveness of Public Services. What policies and procedures need to be designed, or updated/clarified, and then implemented.

1.5.3 Information Assurance—How do we ensure that as Citizen Data is shared it is accurate, safe and secure and only those with a legitimate need to know know it exists or sees it.

1.5.4 Shared Services Common Infrastructure—As we share data and we connect Public Sector organizations together to fulfil the Citizen request how do we ensure that the technology is safe, secure and not prone to "prying electronic eyes".

[245] Steering Committee on Reciprocity.

2. Roles and Accountabilities

2.1 The Accounting Officer for Public Sector bodies however defined are accountable for ensuring that Citizen data is used for the purposes that it was intended for under the various elements of legislation. The Ministry of Justice submission to this Committee sets this out in more detail.

2.2 Accounting Officers are also accountable for ensuring that the appropriate policies, procedures, people and technology are deployed to ensure that at all times Citizen data is protected from rendering it from becoming inaccurate; ensuring that appropriate security policies surrounding the employment of people, the protection of physical access to building and the safety and security of the technology holding Citizen data is at all times maintained to the appropriate standards.

2.3 Accounting Officers are also accountable for ensuring that defined roles and responsibilities exist within their organisations to ensure that necessary risk identification and mitigation strategies are executed to ensure that the safe operational use of Citizen Data is maintained.

2.4 The Ministry of Justice has the accountability for the development and gaining approval, of the Data Sharing Vision, the Data Sharing Strategy and any supporting guidance. The Ministry works closely with the rest of Government and with other relevant parties to ensure that the correct balance is maintained between the rights of the individual to privacy and protection of individuals from terrorism and other crime. Policies and practices are monitored continually by the Government, the Ministry and the Information Commissioner to ensure the balance is in the right place and to prevent abuse.

2.5 The CIO Council's remit is improve the public service delivery by ensuring that the strategic use of technology and computer systems are aligned to the overall government strategy as detailed in the Transformational Government Strategy. Specifically it is:

- 2.5.1 To act as a focus for partnership between IT professionals across government, agreeing and implementing best practice methods, tools and techniques of undertaking IT enabled business change.
- 2.5.2 To bring the Public Sector together by drawing a membership from the wider public sector—central government, local government, and agencies in fields such as health and policing.
- 2.5.3 Charged with creating and delivering a government-wide CIO agenda to support the transformation of government and to build capacity and capability in IT-enabled business change.
- 2.5.4 To balance government-wide agendas with accountabilities in line organisations.
- 2.5.5 Take a holistic approach to the IT enabled change portfolio ensuring where appropriate and possible the Public Sector does not duplicate the creation of technology based systems.

2.6 The Central Sponsor for Information Assurance within the Cabinet Office is accountable for the development of strategy, policy and guidance appertaining to the protection of data including Citizen Data. They are also accountable for ensuring the accreditation of Departmental computer systems and networks has occurred and that they conform to the agreed minimum standards of security, availability and quality.

2.7 Her Majesty's Government Chief Information Officer chairs the CIO Council. His role is to work with departmental CIO's and those undertaking IT enabled change to ensure they are aligned and support the Transformational Government Strategy. In this role, the Government CIO provides leadership to the IT Profession across the wider public sector, enables public service transformation through the strategic deployment of technology, drives the development of shared services and act as the "face" of UK Government IT both home and abroad.

3. The Transformational Government Strategy

3.1 The Transformational Government Strategy set out 13 strands of work that are intertwined and need to be completed if the personalisation of Citizen based services which are convenient to the Citizen are to be delivered. The strategy is not a menu of items that can be picked from that suits the budget, resource or whim of individuals.

For instance:

> There is no point in suggesting that we can personalise Citizen based services if we cannot identify who the Citizen is without any degree of certainty. *The Identity Management Strand.*
>
> If we can identify who the Citizen is, then this is not much use if this basic Citizen Data—that is enough data to execute a Citizen request within another public sector body—cannot be shared. *The Data Sharing Strand.*

> An organisation would be foolish to accept Citizen Data unless they were certain of its quality and provenance. It would be equally foolish for an organisation to share Citizen Data with another organisation unless it had some certainty that the Data would be protected in line with best practice. *The Information Assurance Strand.*
>
> And finally to enable greater certainty over the quality of the computer systems and networks that store and process Citizen Data it is logical to reduce these to a smaller number and share them so that greater investment and protection can be applied to the few rather than spread over the many. *The Shared Services and Common Infrastructure Strands.*

3.2 The CIO Council is the body that looks to ensure that in their departments and in the wider Public Sector the strands of the Transformational Government Strategy are executed.

October 2007

APPENDIX 51

Memorandum submitted by the Department for Transport

1. Executive Summary

Current Activities

1.1 The Department for Transport holds data on drivers, vehicles and vehicle movements.

1.2 The Driver and Vehicle Licensing Agency's (DVLA) has a register containing more than 42 million driver licence records. The drivers' database has personal details—such as name, address, date of birth and driving convictions—for the majority of the adult population in GB. This information is required to check that a person has an entitlement to drive. They also have a register with active records for some 35.5 million vehicles. This holds vehicle keeper information for the UK which is used to collect and enforce vehicle excise duty (VED), and to ensure that vehicles on or off the road are traceable to an individual or organisation.

1.3 Both DVLA and the Vehicle and Operator Services Agency (VOSA) use ANPR Cameras to support their business objectives. DVLA has 15 camera vehicles to identify and take action against those who evade VED. VOSA currently have 8 camera vehicles which are used to identify, stop and investigate commercial vehicles suspected of being used illegally.

1.4 The Highways Agency (HA) operates cameras on England's Strategic Road Network in support of traffic management, eg managing congestion. The cameras fall into two functional categories: Automatic Number Plate Recognition (ANPR) and Closed Circuit Television (CCTV). There are 1,133 ANPR cameras and 1,300 CCTV cameras deployed though precise numbers can vary, for instance because of disruption during roadworks. All data from ANPR cameras operated by the HA is anonymised and the standard feed from CCTV cameras does not produce a picture which is strong enough to identify individuals.

Safeguards

1.4 The Department for Transport takes issues surrounding privacy very seriously. Sharing data to deliver public policy objectives needs to be balanced with protecting privacy and maintaining public confidence that their personal data is adequately protected against misuse.

1.5 It is departmental policy that data sharing should only be undertaken pursuant to specific statutory authorisation, or in other circumstances where a reasonable legal justification has been established (for example implied or ancillary rights pursuant to other statutory functions in combination with residual common law powers). All data sharing must also comply with the European Convention on Human Rights, the Data Protection Act 1998 and the common law duty of confidence.

1.6 A review of data release from the vehicle register to the police and local authorities, and to anyone else that can show "reasonable cause" for requiring it, was undertaken in 2006. This resulted in 14 new measures being implemented to safeguard and protect data from misuse.

2. Data

2.1 The main DfT databases are those held by DVLA which maintains a register of some 42 million driver licence records and a separate register containing active records of 35.5 million vehicles. The information on drivers and vehicles is vital for road safety, and is an essential part of effective enforcement strategies.

2.2 DfT and its Agencies share data with a number of public and private sector organisations, with the necessary controls to safeguard the use of the data and to prevent mis-use. These include:

- police;
- local authorities;

— other Government Departments; and

— private sector.

2.3 Data may be shared for various reasons, including improved customer service and more effective road traffic enforcement. For example:

— the online vehicle licensing system is only possible by linking insurance data, MOT data and DVLA data;

— since 2004, people applying for a new or replacement driving licence no longer need to send in a photograph if they have recently applied for a passport. With the consent of the individual, the passport photo and signature can be used for the driving licence; and

— DVLA data is shared with the police for road traffic purposes, criminal law enforcement and to help identify individuals and the families of those involved in road traffic accidents. Drivers' data is also shared on a case-by-case basis for the prevention, investigation and prosecution of serious crime.

2.4 DVLA is working with North Wales Police to pilot a new scheme which provides direct access to the drivers' register through handheld devices for road traffic purposes. Police are able to confirm the information provided by the driver is consistent with their record on the drivers' register. This initiative will also benefit motorists who do not carry their driving licence as their entitlement to drive can be checked at the roadside, rather than producing their driving licence at their nearest police station.

2.5 It also shares vehicle data with other public sector enforcement agencies, for instance local authorities and Transport for London (TfL) for enforcement of traffic, parking, and London congestion charge offences.

2.6 Data may also be released to other Government Departments. An example of this sharing is with Her Majesty's Revenue and Customs, which is entitled to information under the Taxes Management Act 1970.

2.7 In the private sector the Department shares data with parking enforcement companies and others that can show "reasonable cause" to receive the data, and with car rental companies where the individual gives their consent to the data being shared.

3. Cameras

3.1 The Department and its Agencies utilise ANPR technology to enforce the law against those who evade VED and non-compliant hauliers and bus and coach operators. The great majority of its ANPR and CCTV cameras are used to manage traffic on the strategic road network of motorways and principal trunk roads in England.

3.2 DfT supports the use of police ANPR cameras in their drive to deny criminals the use of the road. In order to help the police target their on-road enforcement against non-compliant vehicles and their keepers, DVLA provides "hotlists" of those vehicles with no VED and also those with no currently registered keeper. Helping the police to target law breakers in this way ensures that the vast majority of law abiding motorists are not troubled.

3.3 DfT is also responsible for policy on safety cameras, though the cameras are owned and operated by Safety Camera Partnerships which are made up of local authorities, police and HM Courts Service in England and Wales.

DVLA ANPR

3.4 DVLA has 15 ANPR camera vehicles in use throughout the UK. These are used either static at the roadside or whilst patrolling on roads to detect unlicensed vehicles. The system is Type Approved by the Home Office and provides photographic evidence of unlicensed vehicles being used on the road. The images are downloaded and used by DVLA to prosecute offenders. The information is used only by DVLA, and if the vehicle is licensed, the information is dropped after 24 hours with no record kept. The on-board computer is updated every 14 days with a new database of unlicensed vehicles. This database is also shared with those Local Authorities and police forces with devolved powers to clamp and impound unlicensed vehicles on behalf of the Secretary of State. It is also shared with VOSA for use with their ANPR vehicles.

VOSA ANPR

3.5 VOSA currently has 8 ANPR camera vehicles in GB. This is due to increase to 21 vehicles shortly. They are used to identify, stop and investigate non-compliant commercial vehicles and those suspected of operating illegally. Their ANPR systems utilise their own intelligence databases and the database of unlicensed vehicles from DVLA.

3.6 VOSA also operate ANPR systems at a number of locations on the motorway network which are linked to weigh-in-motion sensors embedded in the carriageway. The sensors identify overweight commercial vehicles and those suspected of being loaded incorrectly. The ANPR image identifies the suspect vehicle and VOSA officers stop and investigate the vehicle at a safe place on the motorway.

Highways Agency ANPR and CCTV Cameras

3.7 The HA uses ANPR and CCTV cameras to monitor traffic flows and collect anonymised data for traffic management purposes. Currently there are 1,133 ANPR cameras and 1,300 CCTV cameras deployed on the strategic road network, though precise numbers can vary, for instance because of disruption during roadworks.

3.8 As well as monitoring traffic flow, information from the cameras is used to respond to incidents on the network to ensure that travellers have safe, reliable and informed journeys.

3.9 The HA operates two principal ANPR systems—the National Traffic Control Centre (currently 1,033 cameras) and the "Birmingham Box" network of 100 cameras in total including 42 which are operated by the HA. The NTCC cameras are owned and operated by Traffic Information Services Ltd/Serco on behalf of HA through a PFI contract. These will be handed over to HA during 2011. The "Birmingham Box" is split into a network of 42 cameras installed for the M42 Active Traffic Management Project, and of 58 cameras (HA "TAME" project), which have been transferred to the Central Motorway Police Group in the Midlands. The HA do not collect information from these and are no longer responsible for their operation.

3.10 The HA operates 1,300 CCTV cameras, typically at key strategic locations, at regular intervals along the motorway, and at a few locations on the trunk road network, providing real time traffic information to the NTCC and seven Regional Control Centres (RCCs).

3.11 These cameras enable the HA and emergency services to be aware of road conditions and help them deal with real-time traffic flow and incident information quickly and efficiently. As well as management of major incidents and congestion, CCTV cameras also provide a rapid overview of network conditions providing up-to-the-minute information for traffic management services and the media.

3.12 RCCs currently only record CCTV imagery for a variety of pre-determined purposes that could include network asset protection; operational procedures & protocols; incidents occurring on the network; and Health and Safety compliance.

Safety Cameras

3.13 Although DfT is responsible for policy on safety cameras, they are owned and operated by Safety Camera Partnerships in England and Wales. These are made up of local authorities, police and HM Courts Service. From 1 April 2007 local partnerships have greater freedom and flexibility to deploy safety cameras where they are felt to be the appropriate solution to particular road safety problems. The police use their access to DVLA vehicles data to identify the keeper of a vehicle found to be speeding at safety camera sites.

4. Safeguards for Sharing Data

4.1 The Department takes the safeguarding of personal data extremely seriously. Clarity about the legal authority under which data may be shared, including under the Data Protection Act, is critical. The Department also consults closely with the Information Commissioners' Office.

4.2 Where there is regular sharing of data in bulk with other Government Departments and Agencies, for example by DVLA, a Memorandum of Understanding is put in place detailing the principles and responsibilities surrounding the data release. An example of such an arrangement is that with TfL to allow that body to enforce the London congestion charge.

4.3 Other ad-hoc requests for data from other areas of Government are dealt with on a case-by-case basis. These are considered very carefully to ensure the release is lawful and in accordance with DfT policy.

4.4 Following a review of the release of vehicles register information 14 new measures, announced by the Minister for Transport in July 2006, have been implemented. These are designed to protect vehicle keepers from misuse of their information and provide clear and robust complaint procedures where misuse is alleged, while allowing those who do have reasonable cause to get the data they need. Individuals who apply must provide detailed information and evidence to justify their enquiry.

4.5 DfT and its Agencies also have internal controls in place to safeguard the use of data, to ensure that audit trails exist to identify users of data, and to guard against mis-use of data. Breaches of data security are treated very seriously, and where applicable are reported to the Information Commissioner's Office and the police for investigation and action.

November 2007

APPENDIX 52

Supplementary Memorandum submitted by 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 additional evidence are primarily from the data protection perspective.

2. The Commissioner is grateful for the opportunity to provide additional written evidence as the Committee reaches the final stages of the inquiry. In this evidence he sets out the progress made on initiatives he referred to in his earlier evidence and included in his "Surveillance Society Action Plan", reports on other developments taken forward by his office and addresses relevant points raised by other witnesses in their oral evidence sessions.

Privacy Impact Assessments

3. In May the Commissioner issued an invitation to tender, inviting bids from those interested in carrying out research into the experience of using Privacy Impact Assessments (PIA) in other countries, the lessons to be learned from their experiences and the development of a PIA methodology, including a handbook to be used by those wishing to undertake a privacy impact assessment in the UK. The research contract was awarded to a consortium led by Loughborough University and the results of the research project were received on the 31 October 2007. The project deliverables are now being examined and will be published at the Commissioner's planned conference entitled "Surveillance Society: Turning Debate into Action". Further details of this are set out below.

4. In the oral evidence session of Tuesday 12 June a call was made for tougher regulation of IT suppliers and providers.[246] As a similarly useful measure, the Commissioner would welcome a commitment to use privacy impact assessments as part of the OGC Gateway Review Process, thus embedding data protection and wider privacy considerations into the process of setting up any new and substantial government IT system. Not only would this help to ensure that adequate and relevant consideration is given to privacy from the outset, it would also help achieve compliance with the data protection legislation and would go some way towards fostering public trust in the use of their personal information. This approach has been adopted in other jurisdictions overseas and the Commissioner feels there is much merit in adopting a similar approach in the UK.

5. The Commissioner will send a copy of the final PIA research, including an assessment of international experience and the PIA handbook for use in the UK to the Committee as soon as a final version is settled ready for publication and in advance of the general launch in December.

Public Perceptions of the Surveillance Society

6. Another research project currently being undertaken and its results published at the Conference in December is into "Public Perceptions of the Surveillance Society". This research was commissioned in September and the final report is being drawn up by researchers at the present time. Research into public attitudes forms an important aspect of informing our future work in this area. The nature of our work is such that we spend a large amount of time speaking to and meeting with public and private sector organisations about the potential impact of the surveillance society but it is much more difficult to engage with the general public about their perceptions and experiences of it. The research we have commissioned is therefore to explore how aware people are of the different forms of surveillance that intrude into their everyday lives, what their concerns are, what they find acceptable and unacceptable, what they expect and don't expect and what safeguards they think are in place to protect them from unwarranted collection and use of their personal information.

7. Whilst initial findings point towards a general lack of awareness and concern about surveillance society issues amongst the general public, we are keen to try to discover where people feel that the boundaries should be drawn. We are also trying to find out whether they are content with the amount of surveillance taking place in the UK and, if so, whether this is because they feel that the regulations and safeguards surrounding the collection and use of personal information are sufficiently robust to negate any risks to them as individuals.

8. The Commissioner will send a copy of the final report to the Committee as soon as one is available and in advance of the general launch in December.

[246] Q222 Response of Dr Phippen, Lecturer, School of Computing, Communications and Electronics, University of Plymouth.

Surveillance Society: Turning Debate into Action Conference

9. On 11 December 2007 the Commissioner will be hosting a conference following up on the 2006 International Data Protection and Privacy Conference at which he set out to raise awareness about and provoke discussion on the advance of the surveillance society. The December conference—Surveillance Society: Turning Debate into Action will be held at the Bridgewater Hall in Manchester. The Commissioner will use the conference to launch the results of his research projects into privacy impact assessments and public perceptions of the surveillance society. The conference will also look at the technology available to help protect privacy and any necessary changes to the legal and policy framework from a privacy protection point of view. The conference will also examine the practical experience of a government department as it tries to address privacy concerns arising from a major initiative with the Department for Transport outlining its efforts to develop a privacy friendly road pricing scheme.

10. As the title suggests the intention of the conference is to show some practical examples of where action can be or has been taken to address some of the privacy and data protection concerns that the surveillance society raises. Those attending will be provided with information on the privacy impact assessment handbook and will hear how privacy impact assessments operate in other countries.

Information Sharing

11. On 10 October 2007, the Commissioner published his Framework Code of Practice for Sharing Personal Information. The Framework explains how organisations can set up their own arrangements to ensure that where personal information is shared, good practice is adopted. It helps organisations decide when to share information and what information to share, highlights the consequences of sharing and deals with the issue of consent. It is designed to be flexible, enabling organisations to adopt it wholesale or to extract some of its content and integrate this into existing policies and systems. The Commissioner will also be able to endorse the codes of practice created by those using the Framework, subject to him being able to audit and inspect the arrangements.

12. The final version was produced after extensive liaison with relevant stakeholders, both before and during the official consultation period.

13. This is the first time that the Commissioner has produced such a "framework" code, to be adapted and used to suit the needs of those involved in a particular information sharing operation. It reflects the fact that the range of situations in which information sharing can take place is so broad that trying to develop a single prescriptive code, written by the Information Commissioner to be used in all situations, would be unworkable.

14. A copy of the code is attached at Annex A (not printed).

15. The issue of information sharing still continues to provoke wider interest and the Prime Minister has recently announced that the Commissioner and Dr Mark Walport of the Wellcome Trust have been asked to conduct a review of information sharing.

16. The review will look at how information sharing policy should be developed in the future. As part of this, the review may make recommendations on potential changes to the way the Data Protection Act operates as well as setting out recommendations on the powers and sanctions that the Commissioner has available. The final report is due to be published in the first half of 2008.

17. The review terms of reference are attached at Annex B (not printed).

The Revised CCTV Code of Practice

18. The Commissioner first published his CCTV Code of Practice in 2000 and it has proved to be a popular and useful piece of guidance. However, advances in the use of CCTV, both in terms of the number and prevalence of CCTV cameras and the technology available, have meant that some of the references were beginning to become out of date. In order to remain useful, the code needed to be revised to take into account those advances and also to take into account the needs of those operating the systems.

19. Workshops were held with the most relevant stakeholders in this field which helped to determine where they felt revised and/or additional guidance would be of use. The revised code was drawn up and went out for consultation in August. The consultation period ended on October 31 and the Commissioner expects the updated version to be launched in January 2008.

20. Apart from addressing the advances in technology made since the CCTV code was first launched, the new code also amplifies the Commissioner's position with regard to the use of CCTV in particular situations such as recording conversations. It also requires those considering introducing a system to consider the other, less privacy intrusive options before committing to the use of cameras.

21. A copy of the consultation draft is attached at Annex C (not printed) and the final revised version of the CCTV Code of Practice will be sent to the Committee as soon as consultation responses are analysed and a final version agreed.

22. The Home Office and the Association of Chief Police Officers, who were consulted during the revision of the Code have recently published a "National CCTV Strategy" which also reinforces the need for data protection compliance by CCTV operators and suggests greater supervisory powers for the Commissioner.[247] The Commissioner has agreed to participate in a Programme Board set up to take the Strategy recommendations forward.

Commitments Made in the Commissioner's Oral Evidence Session

23. During his oral evidence session, the Commissioner called for a penalty to be introduced into the data protection legislation for situations where there is a flagrant, negligent or repeated disregard of the requirements of the law. He offered to provide further information about this penalty to the Committee.

24. Since the oral evidence session the Commissioner has submitted a draft proposal for changes to data protection powers and penalties to the Ministry of Justice. Once the Commissioner's proposal is finalised a copy will be sent to the Committee.

25. The Commissioner would like to see the creation of a criminal offence of knowingly or recklessly failing to comply with the data protection principles so as to create a substantial risk that damage or distress will be caused to any person. He is also seeking a power to inspect personal data to assess whether or not it is being processed in compliance with the Data Protection Act. He believes that the introduction of such penalties and powers would significantly increase the ability of his office to fulfil its commitment to strengthen public confidence in data protection and to take a risk-based approach to regulation.

26. The penalty would be linked to a failure, knowingly or recklessly to discharge the duty imposed on data controllers under section 4(4) of the Data Protection Act which states that " . . . it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller". The Commissioner is suggesting an unlimited fine for such offences, not a custodial sentence and a defence that the data controller concerned exercised "all due diligence".

27. In terms of powers of inspection, the Commissioner would like to see a broadening of section 54A of the Data Protection Act which relates to the inspection of overseas information systems in which the UK participates such as Europol. He is suggesting that this inspection power should apply to any information system in which personal data are recorded falling within his jurisdiction.

28. Allied to the call for a penalty to be introduced for breaches of the data protection principles, the Commissioner believes that consideration should be given to security breach notification obligations in the UK. These are used in other jurisdictions and involve the organisation which is the subject of a breach being obliged to tell those individuals affected by it such as those whose personal information is involved, as well as, in some cases, the regulator. Such obligatory notifications could, if applied sensibly, not only provide protection for individuals but would also help the Information Commissioner to take appropriate action where necessary.

Points Raised in Other Oral Evidence Sessions

29. In the oral evidence session of Tuesday 12 June 2007 it was suggested that data protection officers in government departments should report to the Information Commissioner rather than to the departmental Parliamentary Secretary.[248] It was felt that this would then ensure that they see their job as enforcing the legislation within the department rather than trying to ensure that the department does not fall foul of the Information Commissioner.

30. Whilst the Commissioner is not in a position to comment in detail on how government data protection officers currently carry out their roles, it is correct that Directive 95/46/EC from which the UK Data Protection legislation is transposed recognises a role for "in-house" data protection officials particularly in relation to notification arrangements (Articles 18 and 20). Such officials are a feature of other countries' data protection regimes such as Germany. Section 23 of the Data Protection Act implements this provision of the Directive by providing for the appointment of "data protection supervisors". The necessary order to bring this section into effect has never been made but this could provide an opportunity to put in place data protection supervisors in government departments and create obligations and duties as additional safeguards, including duties in relation to the Commissioner.

Other Points for Consideration

31. Individuals are increasingly sharing information about themselves with others. The growth of social network sites and online blogs raises the prospect of individuals leaving themselves open to increased surveillance. This not only has an impact on privacy, it also increases that individual's risk of becoming a victim of identity fraud in the future. The Commissioner has already taken some steps to try to help

[247] http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.pdf

[248] Q222 Response of Professor Anderson, Professor of Security Engineering, University of Cambridge and Chair of the Foundation for Information Policy Research.

individuals reduce the risk of identity fraud through the publication of his well-received personal information toolkit earlier this year. The Commissioner is also in the process of drafting guidance for individuals who are using or thinking of using social networking sites. This guidance will be published in the coming months, once comments have been received from the social networking sites involved.

32. The Commissioner's Surveillance Society Action plan does not only concentrate on his own initiatives, it also includes his work responding to the initiatives of others which have surveillance society implications. A significant area of increased state information gathering and analysis is in relation to international travel. The Government now has a well established e-Borders programme and central to this are the information provision and sharing powers in the Immigration, Asylum and Nationality Act 2006. This includes extensive information acquisition and sharing powers for all the UK border control authorities. One of the safeguards put in place to ensure a proper use of these powers is a code of practice on information sharing as required by section 37. The Commissioner has been consulted by the Border and Immigration Agency on a draft and he has made comments that he hopes can be taken into account in the final version before it is laid before parliament.

33. The European Commission has also recently announced the intention to establish a framework decision that will lead to all EU member states acquiring passenger name record details of all airline passengers arriving in the EU. This engages substantial privacy concerns and the Commissioner is working with his EU data protection commissioner colleagues to ensure that this proposal is necessary and if so includes the essential data protection safeguards.

Future Action

34. The Commissioner continues to place great emphasis on work aimed to address surveillance society issues involving the use of personal information. He has recently been consulting on his new data protection strategy and a consultation draft is at Annex D.[249] This makes clear the continued commitment towards dealing with the emergence of a surveillance society. This consultation closed on the 28 September 2007 and the largely positive responses are being analysed in detail.

35. The Commissioner is focussing work on the practical steps that can be taken to deal with the undesirable consequences of a surveillance society and he has a dedicated stream of activities that continue to be managed through his surveillance society action plan. This work has already made substantial progress and he is committed to forging ahead with initiatives to ensure that individuals enjoy a proper level of privacy and data protection and that their personal information is handled in a way that inspires their trust.

November 2007

APPENDIX 53

Memorandum submitted by the Ministry of Justice

Summary

1. The Ministry of Justice (MoJ) is responsible for the Government's domestic, European and international policy on data protection and data sharing. 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 to regulate the processing of personal data under the DPA.

2. The Government published its "Information Sharing Vision Statement"[250] in September 2006. This highlighted some of the ways information is already being shared effectively within the public sector and stated the Government's intention to continue to share information to deliver better services, fight crime and protect public security. The vision recognises that the sharing of personal information must be carried out transparently and with proper safeguards. Within that context the MoJ works with departments to develop policies and deal with data sharing and data protection issues.

Introduction

3. The social and technological advancements of recent years have given citizens greater expectations and opportunities than ever before. They can expect tailored services from the private sector as well as personalised services from government agencies. In order to achieve this the effective and proper use of personal information is needed.

---

[249] Not printed.
[250] "Information Sharing Vision Statement. http://www.justice.gov.uk/docs/information-sharing.pdf

4. Citizens rightly expect that when providing personal information to facilitate the delivery of modern public services and to ensure public safety, that their personal data is secured properly and used appropriately. For example they should expect to see greater individual security through the reduction in crime without unnecessary impingements on their individual privacy or freedoms. The Government's aim is to make sure that information is only shared when there is a benefit to the public and that any information sharing is lawful.

5. 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, for example, avoid citizens having to give repeatedly the same information to a range of service providers.

Collection and Sharing of Personal Information

6. 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. A MORI survey[251] conducted in March this year indicated 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 information sharing.

7. For example, earlier this year, the Department for Work and Pensions (DWP), Her Majesty's Revenue and Customs (HMRC) and local authorities in North Tyneside worked jointly in a trial to speed up the processing of benefits and tax credits to customers in North Tyneside. During the trial the time taken to get all benefits into payment when someone lost their job was halved. The payment of tax credit was stopped more quickly, reducing the possibility of overpayments. Additionally, when customers started work and were entitled to tax credits, the information sharing exercise meant that claimants were switched into the tax credit system promptly. In July this year, the trial was extended to a further six local authorities.

8. Furthermore, in order to prevent and detect crime effectively, including terrorism, the police and other public services can often benefit from access to a variety of sources of data held by the private sector, public authorities and organisations that deliver public functions.

9. 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. New technologies have made possible innovative developments in the public sector such as the Police National Database which, with proper use, will help tackle crime and build public confidence.

10. In Sir David Varney's report[252] 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 recommended a service be developed that would enable members of the public to report changes of circumstances such as births, deaths, and changes of address to Government just once. This information would then be stored in and shared between IT systems designed with inbuilt security and with security of physical access, including specialist training and security checks for staff access.

11. Research[253] 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. 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.

12. Society is rightly concerned that these new developments are being used lawfully and appropriately, with due regard for individual privacy, freedoms and rights. The challenge is to achieve the balance between delivering improved services through better information sharing and protecting the privacy of the citizen from unnecessary intrusion.

13. 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. It is important that the data is adequate, relevant and not excessive for the purposes of sharing and that it is kept only for as long as is necessary for the sharing. These are important protections within the DPA and the European 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.

[251] See *Public Services Policy Review: The Public View*, IPSOS MORI, 27 March 2007 www.ipsos-mori.com/citizensforum/finalreport.pdf

[252] Sir David Varney's review into service transformation *Service Transformation: a Better Service for Citizens and Businesses, a Better Deal for Taxpayers.*

[253] See *Public Services Policy Review; The Public View*, IPSOS MORI, 27 March 2007 http://www.ipsos-mori/citizensforum/finalreport.pdf

14. The Government consults widely on its policy and legislative proposals, affording the public and 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.

15. The Government announced on 25 October that it had invited Richard Thomas, the Information Commissioner and Dr Mark Walport, the Director of the Wellcome Trust to undertake an independent review of the way personal information is shared and protected in the public and private sectors. The review will assess whether in today's society it strikes the right balance between giving people the protection they are entitled to, while allowing them to make the most of the opportunities which are being opened up the by the new information age. The report is expected to be published in the first half of 2008.

The Legal Framework

16. The current legal framework for 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.

17. The DPA regulates the processing of personal data, which is defined widely and includes the collection, use, storage and distribution of personal data. The DPA implements the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and it is underpinned by the ECHR, particularly the right to respect for a private and family life under Article 8, which has been given direct effect in the UK by the Human Rights Act (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 may be possible to share confidential information, for example where it is in the public interest to do so.

18. 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.

19. Under the DPA, organisations and individuals must comply with the data protection principles in order to process personal data unless an exemption applies.[254] 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.[255] 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.[256]

20. 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.[257]

21. Under the DPA, the Information Commissioner is the UK's independent regulator.

Role of the Information Commissioner

22. The Commissioner promotes compliance and good practice, and manages the data protection register and notification by data controllers of details to be held on the register, including the general purposes for which they will be processing personal data. He enforces the DPA and other legislation under which he has powers to act.

23. The Government always keeps under review the mechanisms which regulate and protect the use of personal information 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 and have due regard for his views when developing policy and legislative proposals.

24. The Commissioner's powers under the DPA allow 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.

[254] DPA. s 4(4).
[255] DPA Sched 1, Pt 1, paras 1, 2 and 4.
[256] DPA, Sched 2.
[257] DPA, Sched 3.

25. 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 wherever the case for additional regulatory control is established.

26. 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.

A Case-by-case Approach

27. Effective and appropriate information sharing is not an end in itself. It is one of the foundations for improving services across 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 of Justice has a central role in providing advice on policy and legislative proposals which have an impact upon data protection and data sharing, and to help ensure that all parts of government apply the legal framework consistently.

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 each policy, taking into account technological and social issues relevant to that policy.

29. An example of these are the data sharing provisions of the Serious Crime Act. The Home Office, in close liaison with MoJ, formulated the data sharing provisions of the Act to create a legal gateway through which public authorities can share data for the purpose of preventing fraud, within a framework of appropriate protections. The sharing enabled by the Act must be compliant with the DPA and the Secretary of State is required to produce a code of practice to cover this sharing of information. The provisions also include criminal penalties for the willful misuse of specified data. The effect of the data sharing provisions will be to allow the public and private sector to share information on those attempting to defraud them and prevent further frauds from taking place.

30. Another example is the Order made under the DPA[258] in July 2006. In response to concerns raised, the Secretary of State for the then Department for Constitutional Affairs (now the MoJ) made this Order to facilitate the processing of sensitive personal data provided by law enforcement agencies by payment card issuers in relation to 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 to administer the account relating to that payment card or cancel the card. The MoJ consulted the Information Commissioner before making the order, as required by the DPA. In Parliamentary debate, the Government assured both Houses that the action was fair and balanced; the order was justified and that there would be no prejudice to the innocent party in the case of joint accounts.

32. The Select Committee on the Merits of Statutory Instruments 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?,*[259] the Government is seeking to use the Criminal Justice and Immigration Bill, which was introduced in the House of Commons on 26 June 2007, to amend the DPA to allow custodial sentences where access to personal information has been wilfully or deliberately misused.

34. The Ministry is also working with the Information Commissioner's Office and other Government Departments to assess the need, value and potential use of Privacy Impact Assessments.

Conclusion

35. The Ministry works closely with the rest of Government and with other relevant parties to ensure that the correct balance is maintained between the rights of the individual to privacy and their freedoms and the protection of individuals from terrorism and other crime. Policies and practices are monitored continually by the Government, the Ministry and the Information Commissioner to ensure the balance is in the right place and to prevent abuse. The Ministry welcomes the Committee's inquiry and will respond to issues arising in due course.

November 2007

---

[258] Link to: The Data Protection (Processing of Sensitive Personal Data) Order 2006

[259] 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

APPENDIX 54

Memorandum submitted by the National Policing Improvement Agency (NPIA)

EXECUTIVE SUMMARY

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.

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. NPIA replaced the Police Information Technology Organisation (PITO) and the Central Police Training and Development Authority (Centrex) taking over responsibility for all their functions. It has also taken over policy and/or operational responsibility for some activities for which the Home Office was previously responsible, as well as a number of national projects working directly to ACPO.

3. The NPIA is a policing organisation which 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.

4. 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.

5. The NPIA operates within a strategic framework shaped by the National Policing Board, on which the Agency is represented. Preserving the integrity and probity of these relationships is fundamental to the mission. NPIA aims to be both an enabler of development within the policing community as well as the developer of links beyond policing. These links will support the adoption of proven ideas from research and policing (including internationally). For the Police Service at a national level, NPIA's role is to be the delivery agency.

6. This Memorandum sets out the key areas of NPIA's work considered to be of most relevance to the Committee's Terms of Reference. 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)

7. NPIA's PNC Services is the service provider of the PNC, ViSOR (Violent or Sexual Offenders Register), NFLMS (National Firearms Licensing Systems) 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.

8. NPIA's Data Centre is based in North London. A Disaster Recovery Site is provided within 20 miles and is used operationally to support PNC's 24 hour availability throughout the year. Both sites meet or exceed current security requirements.

9. 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. Of these, approximately six million have a criminal conviction and two million are either CJ Arrestees (ie arrested after the 2003 Criminal Justice Act such that the record of the arrest is held but no charges were brought) or, more recently, with the introduction of the National Firearms Licensing Management System (NFLMS) there will also be Firearms Certificate Holders. The PNC is used to make that information readily available and shared across all Police Forces.

— Drivers, 51 million, where the PNC holds a copy of all driver information held by DVLA, again to make it readily accessible to all Police Forces.

— Vehicles, 57.5 million where PNC holds a copy of all vehicle information for police purposes which is supplemented by operational information eg vehicles of interest or stolen.

— Property, 96,000, where lost property that has a unique serial number is held on PNC so that the information can be shared across all Police Forces.

10. 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.

11. 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).

12. 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

13. 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.

14. 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 12), it has tripartite governance involving ACPO, APA and the NPIA. The Strategy Board is chaired by the ACPO lead on forensic science.

15. 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.

16. The Police and Criminal Evidence Act (PACE)1984, which sets out the rules under which DNA information can be collected is currently being reviewed by the Home Office. This review is designed to ensure that the law is fair, and that it maintains the crucial balance between the usefulness of evidence in police investigations, and the protection of individuals' rights. Proposals will be put out for consultation in Spring 2008.

IMPACT: Information Sharing Between Police Forces

17. The IMPACT Programme, launched as part of the Government's response to the Bichard Inquiry and 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.

18. 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.

19. 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.

20. 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.

21. 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)

22. ANPR technology has been available for over 30 years, although its use in policing was largely restricted to counter-terrorism work until the late 1990's. 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.

23. 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. In the last three years it has delivered two to three times more "offences brought to justice" when compared to conventional policing methods.

24. 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. Currently, the Home Office has retained responsibility for development of the proposals for the wider sharing of bulk ANPR data between third party agencies and the police, and also the process to facilitate of the transfer of bulk Transport for London (TfL) ANPR data to the Metropolitan Police Service (MPS) for the purpose of national security, including terrorism.

Facial Images (Referred to as Facial Mapping in Home Office Memorandum of April 2007)

25. "Facial Mapping" and "Automated Face Recognition" are terms that are frequently used interchangeably but have slightly different meanings. We have assumed that in the context of a "surveillance society" it is really automated Face Recognition (FR) that is primarily of interest here.

26. The police have long been interested in the use of facial images to prevent, detect and solve crime. The proliferation of CCTV cameras in the UK (approx one for every 14 people) means that we are now accustomed to our movements being monitored in this way and for most people this is not an issue. Indeed, if a crime is committed the general public now expect there to be CCTV footage related to the event and concern is expressed on those occasions when it turns out that none is available.

27. The creation of a national facial images database, NPIA's FIND (Facial Images National Database) project, will for the first time enable UK police forces to retrieve and display facial images regardless of which Force Custody Suite originally captured the images. Inevitably FIND also raises the possibility of using automated FR to search this and other databases in conjunction with CCTV or surveillance images (both still and moving images) in an attempt to identify known offenders, terrorist suspects, etc. Recent trials of FR around the world have shown that there is still a long way to go before FR systems will work reliably in such circumstances. Whilst the use of FR is outside the scope of FIND, the NPIA's biometrics team has, for some time, been investigating this area to better understand if, and how, such technology could best be deployed in support of policing.

December 2007

APPENDIX 55

Supplementary memorandum submitted by Department of Health

At the hearing on Tuesday 20 November 2007, I undertook to provide a note about the way in which Health Authorities were handling correspondence from Members of Parliament about their constituents' health affairs. In particular, the Chair asked why Health Authorities had, in his experience, recently begun to seek written confirmation before replying that patients had given their consent to information being provided in response to letters from Members of Parliament.

I have reviewed the guidance currently in issue to the NHS and can confirm that the document "Confidentiality—NHS Code of Practice" advises that—

> "There is a balance to be drawn between ensuring that a patient has understood and properly consented to a disclosure of information and needlessly obstructing an investigation. Careful consideration of any written authorisation and prompt action are key, eg where an MP states, in writing, that s/he has a patient's consent for disclosure this may be accepted without further resort to the patient."

The guidance is designed to ensure that patient confidentiality is protected. Inclusion in correspondence of a reference to the fact that the constituent had given their consent to the matter in question being raised by their Member of Parliament, would help avoid the need for further checks to be made.

November 2007

APPENDIX 56

Supplementary memorandum submitted by the Home Office

At the Committee meeting on 20 November you asked Stephen Hickey, a Department for Transport (DfT) witness, about new proposals that passengers on domestic flights between Northern Ireland and Great Britain will be subject to identity checks. I am replying as this is a matter for the Home Office.

Section 14 of the Police and Justice Act 2006 introduced a new power that will allow the police to capture passenger, crew and service information on air and sea journeys within the United Kingdom. The intention is that the power will be brought into force by secondary legislation in 2008. The specific police requirements under this power, which will include details of the routes affected and data required, are still under discussion within Government. Once the proposals have been finalised they will be subject to a 12 week public consultation.

It is expected that this police power will only apply to air and sea routes between Great Britain and Northern Ireland. People will not be required to use passports, but may be required to produce on of several types of documentation when travelling to enable the carrier to meet the requirements of a police request. Some airlines already request photographic ID under their own conditions of travel to prevent ticket fraud. However all airlines must ensure that it is the same passenger who checks in hold luggage who then boards the aircraft. The police power is designed to be proportionate and reasonable.

We are working very closely with the Republic of Ireland to address the vulnerability in the UK borders from terrorists exploiting the Common Travel Area by attempting to enter the UK via the Irish Republic. The intention is to focus efforts on terrorists and people involved in serious and organised crime. The police will use this data collected under this power to support intelligence led interventions to counter terrorism and tackle serious and organised crime.

The police do use their powers under Schedule 7 of the Terrorism Act 2000 to examine travellers between Northern Ireland and Great Britain. Schedule 7 allows an examining officer to examine and/or detain a person who is at a port or in the border area and (where) the examining officer believes that the persons presence at the port or in the area is connected with entering or leaving Great Britain or Northern Ireland, or their travelling by air within Great Britain or Northern Ireland, to determine whether they are someone who is or has been concerned in the commission, preparation or instigation of acts of terrorism. This power is, however, limited to counter-terrorism issues.

December 2007

APPENDIX 57

Memorandum submitted by Orange UK

1. Introduction

1.1 Orange welcomes the House of Commons Home Affairs Select Committee inquiry into "a surveillance society". With mobile phone penetration at over 80% of the UK population and broadband penetration continuing to grow, the role of electronic communications has become an important factor in building a case of evidence in the fight against crime and terrorism.

1.2 Despite the value of such data, it is vital that government and its agencies meet the right balance between protecting individuals' privacy and accessing data in an appropriate way to help them in their investigations. It is also important that commercial organisations have processes in place to ensure that privacy is protected in meeting the requirements of the Data Protection Act 1998.

1.3 Orange is a key brand of the France Telecom Group, providing mobile, broadband, fixed, business and entertainment services across Europe. It is one of the world's leading telecommunications operators with more than 168 million customers on five continents. In June 2006, Orange merged with Wanadoo, a leading Internet Service Provider (ISP) and now, under a single brand, offers mobile, broadband and multi-play offers, including digital television and home phone services.

1.4 We recognise that, as a leading UK communications provider with over 16 million customers, and as part of the Critical National Infrastructure (CNI), we need to co-operate and assist government and its agencies in their work. Orange has a dedicated Government Liaison, Disclosures & Abuse Management Team that works with both government and law enforcement agencies to provide the necessary information needed to aid an investigation.

2. Data Retention: Civil Liberties v Security

2.1 In line with the Data Protection Act, Orange holds data for as long as is required for business purposes. We have strict processes to protect this data and the privacy of our customers (see below). We are also required to hold specific data as defined and required under the Data Retention (EC Directive) Regulations 2007 (which entered into force on 1 October 2007).for a period of 12 months.

2.2 Orange provides data to law enforcement and government agencies in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA creates a legal and fully regulated basis for the demand by Law Enforcement and Government agencies for the disclosure of subscriber information, itemised billing and other communications data. However, in cases such as dropped 999 calls, we may respond to requests for subscriber details under data protection legislation in order to speed up this process. RIPA also allows for requests to be prioritised in line with the ACPO DCG (Association of Chief Police Officers Data Communications Group) National Prioritisation Grading system. In "life at risk" situations, a request can be made verbally under RIPA, and we will provide real time location information to the requesting agency 24-hours a day. The information is not an exact location but provides a good starting point for the police in their search for a missing or abducted person.

2.3 RIPA places an obligation on the authority requesting the information (and not the organisation which holds the data ie Orange) to prove the proportionality and justification for the request and the subsequent disclosure of the data. Orange is fully supportive of the Single Point of Contact (SPOC) procedure which facilitates the acquisition and disclosure of communications data between service providers and law enforcement agencies. However, we believe SPOCs could be given a higher profile within all law enforcement agencies as communications data becomes more important in criminal and terrorist investigations. We are working with ACPO DCG to address this issue.

2.4 The oversight of these powers is provided by the Interception Commissioner. Orange believes RIPA provides an appropriate balance between civil liberties and security. However, this is an issue that needs to be kept under constant review as technology changes. A careful balance needs to be met between maintaining the privacy of our customers and providing essential data for criminal and terrorist investigations. Orange works within the regulatory framework (see above) to maintain this balance and, whilst we regularly discuss this with government and law enforcement agencies, we believe it is the Government's, rather than a commercial operator's, decision to ascertain whether it adequately meets the balance between security and privacy.

3. Data Protection: Customer Privacy

3.1 Orange takes its responsibility to protect the confidentiality of customer's personal data very seriously. Oversight of this is regulated and enforced by the Information Commissioner and the Government is committed to strengthening its powers to give it access to inspect our processes to ensure we are doing this.

3.2 Orange employs a number of techniques to ensure customers are safeguarded from attempts to fraudulently access account information. We also use a number of processes to monitor our staff's access of customer accounts to ensure such access is warranted. We regularly review and adapt our information security procedures to ensure they are effective.

3.3 Orange is certified to the International Standard for Information Security (ISO27001), and audits are run against this every six months to ensure we are compliant. We therefore continuously monitor, evaluate and improve our controls across the full scope of our business and we have a focus on customer data ahead of any other type of information.

3.4 Orange does not send large amounts of sensitive customer data by internal or external mail. In cases where we have to send data by these methods, the data is generally less sensitive in its nature or composition, or we protect it by encryption techniques for electronic media and by other physical methods for other media types. Most of our data is moved internally by automated transfers between machines and systems, and these transfers are within our corporate perimeter with its security measures. Such flows are protected where appropriate, depending on the type of data and the aggregation of data we need to send, and where such protection can be applied within system limitations.

February 2008

Supplementary memorandum submitted by the Ministry of Justice

Thank you for inviting me to give evidence on 20 November. I hope the Committee found it informative.

In the light of the loss of personal data by Her Majesty's Revenue and Customs, we thought it would be helpful to provide the Committee with written evidence to update the evidence provided in November last. I enclose a further memorandum which I hope the Committee finds helpful.

I also promised during the evidence session in November to look into two matters raised respectively by Mr Davies and Ms Moran. I am sorry for the delay in reporting back to you.

Mr Davies asked what arrangements are in place, if any, for Ministry of Justice and the Department for Work and Pensions to share data about prisoners, in order to ensure that prisoners who abscond from prison do not receive state benefits to which they are not entitled.

The Ministry of Justice and the Department for Work and Pensions (DWP) do indeed share information about prisoners, and do so in compliance with the Data Protection Act, to enable the DWP to check individuals' status to prevent payment of benefits for those serving a custodial sentence. This exchange includes information about people that escape from prison, who are treated as if they are still serving a custodial sentence. I understand that it is rare for absconders from open prisons to attempt to claim social security benefits, as doing so could make their whereabouts known.

An electronic transfer is also sent monthly to the DWP of a further three categories of people:

(i) absconders who are sentenced to custody in their absence;

(ii) those who fail to attend court where they have appealed against a custodial sentence; and

(iii) escapees.

Since July 2007, the Ministry of Justice has provided a total of five names to DWP in the first two categories. None were in receipt of any state benefits. The third category is quite specific, and concerns people who have escaped in transit from the court to prison. There have been four occurrences since July 2007 and none were in receipt of benefit.

Ms Moran mentioned that earlier last year CCTV footage of an incident in Luton town centre had been posted on the Internet. I reported to the Committee that any breaches of the Data Protection Act are for the Information Commissioner to investigate and prosecute where necessary. I have therefore referred the matter to Richard Thomas and he has assured me that he will investigate.

The Commissioner's investigation will probably take quite some time to conclude and he may not be able to report the outcome publicly. However I hope my letter reassures the Committee that the matter will be thoroughly investigated.

1. 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 the use of personal data in the public and private sectors. The review is considering 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. It will include recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection. It will also make recommendations how data sharing policy

should be developed in a way that ensures proper transparency, scrutiny and accountability. Public consultation on these issues was opened on 12 December 2007 and closed on 15 February 2008. The report and recommendations will be submitted to the Justice Secretary in the first half of 2008.

2. On 22 November 2007, following the loss of data by HMRC, the Prime Minister invited the Information Commissioner to undertake spot checks of Central Government Departments' compliance with the Data Protection Act and the data protection principles. These spot checks are expected to commence in Spring 2008. The ICO anticipates undertaking inspections of three or four Departments over the coming months. A report containing recommendations to improve its data handling procedures will be provided to each Department at the end of each assessment.

3. Also on 22 November, the Prime Minister asked the Cabinet Secretary, Sir Gus O'Donnell, to undertake a review of the data handling procedures of Departments and agencies. The first stage, which concluded on 10 December, involved Departments undertaking an analysis of their systems and procedures for complying with policies and standards on data protection, including making recommendations for practical improvements. An interim progress report, *Data Handling Procedures in Government: Interim Progress Report*, was published on 17 December 2007. This report made several recommendations for data security and protection going forward including:

— ensuring that Departments are clear about roles, responsibilities and minimum standards that they must apply,

— reinforcing the culture across the public service that values and protects information and people's privacy, and

— ensuring that performance is transparent and the right external scrutiny mechanisms are in place to promote improvements into the future.

Initial cross-Government recommendations relating to the framework within which data is handled included:

— enhanced transparency with Parliament and the public about action to safeguard information and the results of that action, through Departmental annual reports and an annual report to Parliament,

— increased monitoring of information assurance through, for example, Accounting Officers' Statements on Internal Control,

— improved guidance to those involved in data handling, that is simplified and better tailored, setting clear common standards and procedures for departments on data security,

— legislative steps to enhance the ability of the Information Commissioner to provide external scrutiny of arrangements across the entire public sector through "spot checks", and

— commitment in principle to provide for new sanctions under the Data Protection Act for the most serious breaches of its principles.

Government will be issuing a consultation document on the last two recommendations shortly.

4. A further review commissioned by the Prime Minister on 22 November 2007 was that of HMRC's data handling procedures undertaken by Kieran Poynter of PricewaterhouseCoopers. The interim report, which was published in December 2007, set out the work Kieran Poynter had already undertaken and made recommendations for immediate steps for HMRC to take to protect data security. They included: the imposition of a complete ban on the transfer of bulk data without adequate security protection, such as encryption; measures to prevent the downloading of data without adequate security safeguards, and disabling personal and laptop computers to prevent downloading of data on to removable media. A full report is expected in Spring 2008.

26 March 2008

Supplementary memorandum submitted by the National Policing Improvement Agency

I undertook at the Home Affairs Select Committee on Tuesday 18 March 2008 to write to you about the number of people on the National DNA Database (NDNAD), the reasons for retaining DNA samples and profiles from persons who have been arrested and sampled, but not charged or convicted, and about the number of matches between crime scene profiles and profiles retained from people who have been arrested, but not convicted.

2. On 31 December 2007, there were 4,920,703 subject profiles on the NDNAD from all forces (England, Wales, Scotland and Northern Ireland). The number of profiles held on the database is not the same as the number of individuals. As it is possible for a profile to be loaded onto the NDNAD on more than one occasion, some profiles held on the NDNAD are replicates. This can occur, for example, if the person provided different names, or different versions of their name, on separate arrests, or because profiles are upgraded. Therefore this number of profiles represents an estimated 4,264,251 individuals from all forces.

3. Information on whether persons with a DNA profile on NDNAD have been convicted/not convicted of an offence is not held on the DNA database, but is available from the Police National Computer (PNC). It is not possible to give a precise figure for the number of persons with a DNA profile on the NDNAD who have committed no offence as some relevant conviction and caution records have been weeded from the PNC. However, on 31 October 2007, there were an estimated 3,938,000 persons on the NDNAD who had been sampled by police forces in England and Wales, of whom 3,637,163 persons had a record retained on PNC. Of these, 3,117,942 persons had a conviction, caution, formal warning or reprimand recorded on the PNC (79% of persons on the NDNAD sampled by forces in England and Wales); and 519,221 persons (13% of persons on the NDNAD sampled by forces in England and Wales) had no current conviction, caution, formal warning or reprimand recorded on PNC.

4. The 519,221 figure includes some persons who may have had a caution or conviction record removed from PNC after five to 10 years in accordance with the Rules for Criminal Record Weeding (which applied prior to April 2006); persons who have been charged and acquitted or proceedings discontinued; persons who have been charged with a recordable offence and proceedings are on-going; and persons who have been arrested but no further action was taken against them. The PNC records for the other 300,993 persons (8% of persons on the NDNAD) had been removed from the PNC for various reasons, for example, their conviction and caution records had been weeded after five to 10 years, the person had been acquitted or proceedings were discontinued.

5. Prior to 2001, the police could take a DNA sample from anyone charged with a recordable offence, but it had to be destroyed if charges were dropped or the person was found not guilty. The Criminal Justice and Police Act 2001 changed this so that DNA could be kept from those who had been charged even if they were acquitted. These provisions have been challenged in, and fully considered by, the UK courts. In 2002, two persons (S, a juvenile, and Marper) challenged whether the retention of fingerprints, DNA samples and profiles under the Criminal Justice and Police Act 2001 of persons charged with, but not convicted of, a criminal offence, constituted an interference with their rights under Articles 8 (right to privacy in private life) and 14 (prohibition of discrimination on any grounds eg sex, race) of the European Convention on Human Rights. In July 2004 the House of Lords found that the retention provisions were proportionate and justifiable and not in breach of the European Convention on Human Rights.

6. The UK courts recognised that the retention of samples and DNA profiles involves a triangulation of interests. Lord Steyn commented that the privacy of those subject to the DNA data is not the only issue at stake. The purpose of the criminal law is to permit everyone to go about their daily lives without fear of harm to person or property. And it is in the interests of everyone that serious crime should be effectively investigated and prosecuted. There must be fairness to all sides, which involves taking into account the position of the accused, the victim and his or her family, and the public.

7. The applicants subsequently appealed to the European Court of Human Rights. The case was heard in the ECHR Grand Chamber at a public hearing on 27 February 2008. The Judgment will be available later this year, possibly in the summer.

8. The retention of samples, DNA profiles and fingerprints has demonstrable benefits for policing but does not have any practical consequences for individuals, unless their DNA profile matches with a DNA crime scene profile. The retention of DNA records is no different to holding other forms of identification information. There is no personal cost or material disadvantage to the individual simply by being on the DNA database. It is an information database and not a criminal database. Inclusion on the DNA Database does not signify a criminal record and does not imply that a person is an offender. It does not hold any information about criminal records and does not affect applications for jobs or visas for foreign travel.

9. The Police and Criminal Evidence Act 1984 provides safeguards governing the use of retained samples and profiles. This specifies that DNA samples and profiles may only be used for the purposes of the prevention and detection of crime; the investigation of an offence; the conduct of a prosecution; or the identification of a dead person. As a result of these provisions, the use of retained material is strictly controlled, and there have been no cases of misuse of data retained on the DNA database to date.

10. A DNA profile is simply a sequence of numbers and is obtained by analysing some of the non-coding or "junk parts" of the DNA sample. These parts do not contain genetic information. DNA profiles therefore contain very little, if any, material information about an individual's medical history or disease liabilities. It is the sequence of numbers which is held on the National DNA Database. The use of the retained profile only occurs when an automated search of the database occurs. If a match occurs, the matched record is identified and the details for that record revealed: the name of the individual and a limited amount of personal information attached to that record (gender, date of birth, sampling force etc). The identifying details may then be used in the criminal investigation of the crime, either to rule out innocent parties, or potentially identify the real perpetrator of a crime. In the absence of a match, the storage of their records has no practical consequence for the individual.

11. The power to retain DNA from persons arrested and not convicted therefore maintains an appropriate balance between the rights of the citizen and their freedom from arbitrary interference and ensuring that the police have sufficient powers to tackle crime and deal with offenders on behalf of the wider community.

12. Research shows that in the period May 2001 to December 2005, an estimated 200,000 DNA samples taken from people charged with offences were retained on the National DNA Database, which would previously have had to be removed because of the absence of a conviction. From these, approximately 8,500 profiles of individuals were matched with crime scene profiles during that period, involving nearly 14,000 offences. These offences included 114 murders, 55 attempted murders, 116 rapes, 68 sexual offences, 119 aggravated burglaries and 127 of the supply of controlled drugs.

13. The Criminal Justice Act 2003 (which came into force in 2004) extended police powers further so that DNA could be taken and retained from anyone arrested for a recordable offence and held in a police station. Research carried out in the period April 2004 to December 2005, shows that the retention of DNA profiles of arrested persons who had not been charged or proceeded against had resulted in matches with crime scene profiles from over 3,000 offences including 37 murders, 16 attempted murders and 90 rapes.

14. These are real cases where the police have been provided with a lead in serious crimes, and future crimes no doubt prevented, because of the retention of DNA evidence on the database which would previously have been destroyed. To give a real case example:—"AA" was arrested in February 2005 for alleged violent disorder at his home. He had a DNA sample taken and added to the DNA database and was later released without charge. In July 2005, a stranger rape occurred 25 miles away from "AA"s home. The only clue was a DNA crime scene profile obtained from skin beneath the victim's fingernails. The profile was searched against the NDNAD and generated a match with "AA"s DNA profile. There were no other leads to solve the crime; the DNA evidence proved vital in detecting "AA" as the offender. He was jailed for six years for sexual assault.

15. "Matching" means DNA taken from a crime scene matches that from a person whose profile is on the NDNAD—in other words, a match is information pointing to a person's presence at a crime scene, and does not necessarily indicate guilt as a person may have had legitimate access to the scene. "Detections" are crimes with a DNA match which were cleared up by the police. In 2006–07, there were 41,717 crimes with DNA matches. Of these, 19,949 were classified by police forces as detections. However, there were a further 21,199 indirect detections in that year—that is, crimes detected as a result of further investigation linked to the original offence, for example because an offender on being presented with DNA evidence of his involvement in an offence also confesses to other offences.

1 April 2008

Further supplementary memorandum submitted by the Home Office

Mr Salter asked a question about the debate on the retention and use of DNA data in relation to the current review of the Police and Criminal Evidence Act (PACE). I thought that I should clarify the position in relation to the timescales involved. As I indicated, we are aiming to launch the final public consultation in relation to the PACE Review in the Spring. However, I should add that, as you may know, there is a case currently under consideration by the ECtHR (*S and Marper v United Kingdom*) in which the applicants are challenging the policy of retaining fingerprints and DNA from those acquitted or where no further action was taken. The hearing took place in February. While timing of the Judgement is a matter for the court, I understand that it is not expected before the Summer. We will need to consider future policy in this area in the light of that Judgement, so we will not be putting forward proposals in this area when we consult on the PACE Review in the Spring. Instead, we will be setting out proposals on retention of biometric data in a separate consultation exercise in the light of the ECtHR Judgement and comments received on this issue in response to the PACE Review process.

4 April 2008

Memorandum submitted by Caspar Bowden

Privacy Enhancing Technologies (PETs) span disparate fields of computer science research[263] (eg the cryptography of "private credentials", untraceable and unlinkable data transport mechanisms, biometric encryption, human-computer interaction and usability, policy control languages, database/statistical privacy) which in combination can create complete "privacy systems". PETs should not be considered to be a "toolbox" which can rectify specific privacy problems in isolation.

Industry and academia are able and willing to develop effective PETs and privacy systems, but there is a chronic lack of awareness and interest from both data controllers and most regulators. Since data protection compliance obligations fall on data controllers, in the absence of clear incentives (regulatory or economic) to deploy PETs, it is unreasonable to expect them to become widespread through market forces or regulator

[263] Digital Privacy: Theory, Technologies, and Practices: Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, Sabrina di Vimercati eds, Auerbach 2007.

exhortation alone. Sanctions sufficient to deter organisations from treating breaches of information privacy as an acceptable business contingency, and greater public awareness of privacy risk are probably necessary to generate market demand.

Design issues in identity systems and privacy systems are really complementary and inseparable—and they require "threat modelling" of risks both to the individual and organisations—which are not necessarily similar or symmetrical. However the DP principle that processing should not be "excessive" in relation to specified and legitimate purposes is crucial for reconciling conflicting interests, but the policy of the ICO to date has generally eschewed major interventions to halt disproportionate processing,[264] in contrast to some other European DPAs. The policy climate for discussion of enterprise information security in the US has been profoundly affected by the broad scale of security breaches that have come to light, since the passage of security breach disclosure laws, however the ICO remains ambivalent whether individuals have a right to be informed.

Privacy is often fatally compromised in designs for large scale identity systems through preconceptions that all transactions need ultimately to be traceable or (re-) identifiable, extreme hypothetical cases used to justify overbroad processing of personal information, and reliance on procedural rather than technical safeguards. Sophisticated PETs can provide much more robust bulwarks against function-creep than policy controls alone, but it must be understood that the purpose of these technologies is expressly to minimize the disclosure of personal information to the absolute minimum required.

Advanced PETs for identity management have some very curious properties, which have been painstakingly designed by a small number of world-class cryptographers over the past twenty years, to try and achieve better outcomes for both security and privacy. However the subtlety of the problems these techniques are designed to solve can seem very abstruse to non-specialists, and the techniques themselves can accomplish things which might seem logically impossible, or contrary to the intuition of the layperson.

For example, it is possible to authenticate a transaction in such a way that if a cryptographic token (which proves entitlement to some service) is used only once (ie honestly and as intended), it can be mathematically guaranteed that the individual cannot be identified. However if an attempt is made to forge or copy a token, or use it more than once, then only in that contingency does it become possible to trace and identify the person to whom it was issued.

The above idea was essentially conceived as a way of implementing online payment services with the privacy properties of cash. A more recent and much more widely applicable technique is the ability to revoke the validity of long-lived untraceable tokens with service providers other than those that issued the tokens, without the necessity to identify the owner of the token.

There is now a family of such innovative cryptographic techniques which together constitute a very powerful new paradigm for combating fraud and abuse, whilst strongly preserving the privacy of honest users. It means that privacy is compromised if and only if dishonesty is detected, and thus potentially forms the basis of a new kind of social contract with citizens. The potential applications include:

- road-pricing and congestion charging;
- welfare benefits, healthcare, and social services entitlement;
- private sector use of data from the National Identity Register; and
- use of a national identity card in over-the-counter transactions.

The fundamental legal and policy issue this raises is that if one takes the Human Rights Act (and Art.8.1 of ECHR) seriously, the state has a duty to limit intrusions into privacy to that which is necessary, not in a general sense, but case-by-case according to the circumstances of the individual. Therefore the use of these advanced PET techniques is mandated by the HRA (subject to reasonable feasibility), because it infringes privacy only to an extent that is individually proportionate. This is in stark contrast to schemes (such as the Oyster card) which rely on blanket collection of identifiable transaction data, and thus are highly vulnerable to "function creep".

As things stand, in systems which collect all transactional data identifiably (on the basis that it cannot be predicted in advance which transactions may need to be retrospectively traced for fraud investigation), a "side-effect" is that a database of all transactions is retained (for some period), but because the database exists, it is a temptation to use it for general surveillance or other purposes unrelated to its primary function.

However, to see the connection between human rights and these advanced technologies, one has to appreciate both the counter-intuitive possibility of such "conditional identifiability", and the implications of existing ECHR jurisprudence. So far, no parliamentary inquiry in any ECHR jurisdiction has spanned this legal and technical gulf. Policy makers are simply unaware these technical possibilities exist. Thus the legality of blanket retention of identifiable transaction data is never fundamentally questioned, because there seems to be no logical alternative to providing a realistic capability for audit and fraud control.

This is the main point I would wish the Committee to consider in this inquiry. However I would also make the following recommendations for specific reform of the Data Protection Act 1998.

[264] The affair of fingerprinting at Heathrow Terminal 5 is a rare exception.

— The right of the data subject to access their personal data should in general be exercisable online and without charge. I have more detailed proposals for the necessary technical and policy reforms.

— The definition of personal data in S1, which presently might exclude data which is only "indirectly" identifiable from being personal, should be altered to implement fully Recital 26 of the Directive ("or by any other person").

— There should be a presumption that the consent of the data subject is required for processing personal data, with the onus on the controller to specify why derogation from obtaining consent is justified. Essentially the emergence of user-centric identity management technologies makes this feasible. In previous pre-Internet decades of data protection policy it would not have been feasible.

Disclosure: although I am submitting this memo as a private individual, and not to represent the views of my employer, I feel it is proper to disclose that between the time this note was initially drafted and later finished, Microsoft has (partially in consequence of my recommendations) acquired the intellectual property of Credentica Inc, and hired Dr Stefan Brands, one of the leading cryptographers in the field of advanced PETs.

8 April 2008

Further supplementary memorandum submitted by the Home Office

Thank you for inviting me to give evidence to the committee on 18 March. During my evidence session I was asked to provide you with a note to clarify the timescales for the revision of the RIPA codes and the two reviews which I mentioned during the course of my evidence.

Timeline for Delivery of Revised RIPA Codes of Practice

The Home Secretary in her statement to Parliament on 21 February gave an undertaking to deliver a revised Covert Surveillance and Covert Human Intelligence Sources Code of Practice by December 2008.

The review of the Codes has already started. A number of issues have been identified on which we will need to consult with our stakeholder community to ensure both that they have the powers that they require, and that appropriate oversight mechanisms are in place without adding unnecessary bureaucracy. The stakeholder community with an interest in surveillance activity is wide ranging and includes law enforcement, intelligence agencies, public authorities, the Office of Surveillance Commissioners, the Information Commissioner, Law Society, Bar Council, prosecutors, community groups and Human Right organisations. We intend to publish the draft codes for consultation over the summer.

Both Codes are subject to the affirmative resolution in both Houses, so we will be seeking to lay the revised codes before Parliament in the Autumn.

Internal Home Office Review

In the first Home Office corporate strategy for information, systems and technology published in February 2007 as part of the Reform Programme, Information Assurance was recognised as one of the top cross-cutting thernes It will continue to feature prominently in the updated strategy currently being developed.

A review was initiated in August 2007 to assess the current situation, establish any requirements for change and identify any actions to be taken. This review was not initiated in response to an incident or problem, but reflects the Home Office's proactive approach to protecting information. The review is led by a Government independent Reviewer, Nick Coleman, who recently undertook a review of information assurance across government for the Cabinet Office.

The first phase of the Home Office Information Assurance Review has now been completed and resources have been put in place within the Office of the CIO to implement the recommendations. The next phase of the review is under way and it is estimated that the full review and implementation will be completed by March 2009.

Hannigan Review

The Home Office, along with all other departments, took part in the Cabinet Office review of Data Handling Procedures in Government, announced by the Prime Minister on 22 November and led by Robert Hannigan. This review has now produced a set of mandatory standards and the Home Office is using the same Implementation Programme to implement the requirements of both this and the Coleman review. Early work on the implementation of the mandatory standards has already begun and all implementation work is due to be completed by the end of the 2008–09 Financial Year.

18 April 2008

Supplementary memorandum submitted by the Law Society

We are writing to you in the light of the announcement that the Committee will be considering the implications of the Rose Report dealing with surveillance issues at HM Woodhill prison as part of your Surveillance Society Inquiry.

The Government inquiry by Sir Christopher Rose will deal with the issue of the bugging of MPs. As you know, since the announcement of this inquiry there have been allegations of systematic bugging of solicitors and their clients at Woodhill. These latter allegations would appear to be outside the terms of reference of Sir Christopher's inquiry as announced by the Lord Chancellor and Secretary of State for Justice, the Rt. Hon Jack Straw MP, in the House on 4 February. They are, in our view, equally serious.

The President of the Law Society, Andrew Holroyd, has now written to Jack Straw (with copies to the Home Secretary and the Attorney General) to explain that if these allegations prove to be true the practice is completely unacceptable and an affront to the rule of law. We have asked for assurance that such monitoring has not taken place or that if it has, it has now ceased. Should it have occurred, we have asked for information about its prevalence.

We have also raised a wider issue that we believe will be of concern to the Committee in its inquiry into the Surveillance Society—the unsatisfactory nature of the current legislative framework. Our concern is not only the absence of explicit statutory safeguards for legal professional privilege under the Regulation of Investigatory Powers Act 2000 but the overall complexity of the Act and its interaction with other legislation, including the Anti-Terrorism Crime and Security Act 2001. This latter point was the subject of our Memorandum of Evidence to the Privy Council in 2003. As well as enlarging the scope for deliberate abuse it may well be that such complexity creates operational difficulties and could lead to genuine but serious mistakes. The consequences of deliberate abuse or serious mistake can be severe. In 2005 for example, the Court of Appeal overturned a conviction for murder on the grounds that bugging privileged conversations between a solicitor and their client undermined the rule of law.

Our view is that a confused and complex legislative framework for surveillance, along with equally complex and overlapping oversight arrangements, are significant and dangerous components of a Surveillance Society. Clear laws and the right to unmonitored and privileged legal advice are fundamental to any free society.

20 February 2008

Printed in the United Kingdom by The Stationery Office Limited
6/2008 378100 19585