HOUSE OF LORDS

Select Committee on the Constitution

2nd Report of Session 2008–09

Surveillance: Citizens and the State

Volume I: Report

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

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 18–I

Select Committee on the Constitution

The Constitution Committee is appointed by the House of Lords in each session with the following terms of reference:
To examine the constitutional implications of all public bills coming before the House; and to keep under review the operation of the constitution.

Current Membership

Lord Goodlad (Chairman)
Lord Lyell of Markyate
Lord Morris of Aberavon
Lord Norton of Louth
Lord Pannick
Lord Peston
Baroness Quin
Lord Rodgers of Quarry Bank
Lord Rowlands
Lord Shaw of Northstead
Lord Wallace of Tankerness
Lord Woolf

Declaration of Interests

A full list of Members' interests can be found in the Register of Lords' Interests:
http://www.publications.parliament.uk/pa/ld/ldreg/reg01.htm

Publications

The reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee are available on the internet at:
http://www.parliament.uk/hlconstitution

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at
www.parliamentlive.tv

General Information

General Information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at:
http://www.parliament.uk/parliamentary_committees/parliamentary_committees26.cfm

Contact Details

All correspondence should be addressed to the Clerk of the Select Committee on the Constitution, Committee Office, House of Lords, London, SW1A 0PW.
The telephone number for general enquiries is 020 7219 1228/5960
The Committee's email address is: constitution@parliament.uk

CONTENTS

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

References in the text of the Report are as follows:
(Q) refers to a question in oral evidence
(p) refers to a page of written evidence

Surveillance: Citizens and the State

CHAPTER 1: INTRODUCTION—THE COMMITTEE REPORT

Background

1. Surveillance is an inescapable part of life in the UK. Every time we make a telephone call, send an email, browse the internet, or even walk down our local high street, our actions may be monitored and recorded. To respond to crime, combat the threat of terrorism, and improve administrative efficiency, successive UK governments have gradually constructed one of the most extensive and technologically advanced surveillance systems in the world. At the same time, similar developments in the private sector have contributed to a profound change in the character of life in this country. The development of electronic surveillance and the collection and processing of personal information have become pervasive, routine, and almost taken for granted. Many of these surveillance practices are unknown to most people, and their potential consequences are not fully appreciated.

2. Commenting on these developments in August 2004, the Information Commissioner Richard Thomas warned against the possibility of the UK sleepwalking into what he referred to as a "surveillance society".[1] In particular, he expressed concern about a raft of new Government proposals, including the establishment of a national identity card scheme, and the creation of a database containing the name and address of every child under the age of 18.

3. The years that have followed these comments have seen an expansion in the National DNA Database (NDNAD), the introduction or development of new databases for a variety of public services, and a steady increase in the use of CCTV in both the public and private sector. There has been a profound and continuous expansion in the surveillance apparatus of both the state and the private sector. In the past, computer databases and data sharing, the monitoring of electronic communications, electronic identification, and public area CCTV surveillance were relatively uncommon. Today these technologies are ubiquitous and exert an influence over many aspects of our everyday lives. The expansion in the use of surveillance represents one of the most significant changes in the life of the nation since the end of the Second World War, and has been shaped by a succession of governments, public bodies, and private organisations. Furthermore, surveillance continues to exert a powerful influence over the relationship between individuals and the state, and between individuals themselves. The selective way in which it is sometimes used threatens to discriminate against certain categories of individuals.

4. In 2006, the Information Commissioner commissioned the Surveillance Studies Network to compile *A Report on the Surveillance Society*. The Report was published in November 2006, and focused on surveillance in everyday

---

1 Ford R, "Beware rise of Big Brother state, warns data watchdog", *The Times*, 16 August 2004.

life in the UK today and in the future, and on how it might be regulated.[2] In March 2007, the Royal Academy of Engineering (RAE) produced its report, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, which also made a number of recommendations for regulation.[3]

5. In the light of these developments, we decided to undertake an inquiry into "the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State." The then Chairman, the late Lord Holme of Cheltenham, said that "the broad constitutional implications of these changes have not thus far been sufficiently closely scrutinised. As a Committee we hope to get to the bottom of how these changes are altering the relationship between individuals and the State, and to ascertain whether necessary protection is in place."[4] We pay tribute to Lord Holme, not only for his influence in launching this inquiry, but for his wise counsel in chairing the Committee from 2004–2007.

6. Some of the questions we sought to answer included:

- Have increased surveillance and data collection by the state fundamentally altered the way it relates to its citizens?
- What forms of surveillance and data collection might be considered constitutionally proper or improper? Is there a line that should not be crossed? How could it be identified?
- What effect do public and private sector surveillance and data collection have on a citizen's liberty and privacy?
- How have surveillance and data collection altered the nature of citizenship in the 21st century, especially in terms of citizens' relationship with the state?
- Is the Data Protection Act 1998 sufficient to protect citizens? Is there a need for additional constitutional protection for citizens in relation to surveillance and the collection of data?

7. We acknowledge that many of these questions are far reaching, and that finding answers to them may not be easy. We recognise that no single government bears sole responsibility for the concerns raised in this report, and that the solutions which we propose will require commitment from politicians of all political persuasions, and from other groups in the public, private and voluntary sectors, if we are to respond effectively to the challenges posed by surveillance and data collection.

Developments during the course of the inquiry

8. During the course of the inquiry, a number of reports were published by the Government, commissioned experts, think tanks, campaign organisations, and other Parliamentary Committees. In addition, a number of high profile news stories drew attention to the issues which we were examining. Box One

---

2 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report*, for the Information Commissioner, September 2006.

3 The Royal Academy of Engineering, Dilemmas of Privacy and Surveillance: Challenges of Technological Change, March 2007.

4 http://www.parliament.uk/parliamentary_committees/lords_press_notices/pn260407const.cfm

highlights a selection of these developments, which we discuss in more detail below.

9. The news stories have been subject to a substantial amount of media coverage and analysis by a wide range of journalists. Television programmes, such as *Panorama*, have highlighted surveillance in its many varieties. Websites and "blogs" have been very active with commentary on stories, policies and developments. In addition, campaign groups have sought to raise public awareness and exert influence on the policy process.

BOX 1

Timeline of main events

- July 2007. Establishment of the National DNA Database Ethics Group, chaired by Professor Peter Hutton. The Group held its first meeting in September 2007, and published its First Annual Report in April 2008.[5]
- September 2007. Publication of the Nuffield Council on Bioethics Report on *The Forensic Use of Bioinformation: Ethical Issues*.[6]
- October 2007. The Prime Minister asked the Information Commissioner, Richard Thomas, and Mark Walport, Director of the Wellcome Trust, to "undertake a review of the framework for the use of information".[7]
- October 2007. Publication of *Overlooked*, Liberty's report on privacy and surveillance.[8]
- October 2007. Publication of the Home Office/ Association of Chief Police Officers (ACPO) *National CCTV Strategy*.[9]
- November 2007. The Government announced that the child benefit details of 25 million people had been lost after an Her Majesty's Revenue and Customs (HMRC) computer disc went missing, and that Kieran Poynter, the then Chairman and Senior Partner of PricewaterhouseCoopers, would undertake a review of HMRC's security procedures.[10] The Cabinet Secretary, Sir Gus O'Donnell, was asked to undertake a review of data handling procedures in government.
- December 2007. It was revealed that a computer hard drive with the details of 3 million UK learner drivers had gone missing in the USA, and that the details of 7,500 vehicles and their owners had been lost by the Driver and Vehicle Agency (DVA) in Northern Ireland.[11]
- January 2008. Publication of the House of Commons Justice Committee's report on *Protection of Private Data*.[12] The Government's response was published in March 2008.[13]

---

5 1st Annual Report of the Ethics Group: National DNA Database, April 2008.

6 Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues*, September 2007.

7 Gordon Brown MP, Speech on Liberty, 25 October 2007.

8 Gareth Crossman, Liberty, Overlooked: Surveillance and Personal Privacy in Modern Britain, October 2007.

9 Home Office and ACPO, *National CCTV Strategy*, October 2007.

10 HC Deb 20 Nov 2007 cols 1101–04

11 HC Deb 17 Dec 2007 cols 624–26

12 1st Report (2007–08): *Protection of Private Data* (HC 154).

13 3rd Special Report (2007–08): Protection of Private Data: Government Response to the Committee's First Report of Session 2007–08 (HC 406).

- January 2008. It was announced that the Ministry of Defence had lost the details of 600,000 Royal Navy recruits when a laptop was stolen, and that Sir Edmund Burton, Chairman of the Information Assurance Advisory Council, had been asked to undertake an inquiry into the data loss.[14]
- February 2008. Media reports alleged that covert surveillance of two visits by Sadiq Khan MP to a prisoner had been undertaken.[15] The Chief Surveillance Commissioner, Sir Christopher Rose, was asked to undertake an inquiry. His report was published later that month.[16]
- March 2008. Publication of the report of the Joint Committee on Human Rights (JCHR) on *Data Protection and Human Rights*.[17] The Government's response was published in June 2008.[18]
- April 2008. Media reports expressing concern at the use of surveillance powers by local authorities under the Regulation of Investigatory Powers Act 2000 (RIPA), in particular in relation to suspected fraudulent school place applications.[19]
- April 2008. Publication of Sir Edmund Burton's *Report into the Loss of MOD Personal Data*.[20]
- June 2008. Publication of the report of the House of Commons Home Affairs Committee on *A Surveillance Society?*[21] The Government reply was published in July 2008.[22]
- June 2008. Publication of Sir Gus O'Donnell's *Data Handling Procedures in Government: Final Report*, undertaken in the wake of the HMRC data loss.[23]
- June 2008. Publication of Kieran Poynter's *Review of Information Security at HM Revenue and Customs: Final Report*.[24]
- July 2008. Publication of the Thomas-Walport *Data Sharing Review Report*.[25] The Government response was published in November 2008.[26]
- December 2008. In the case of *S. and Marper v. The United Kingdom*, the European Court of Human Rights ruled that keeping the DNA profiles of individuals not convicted of a criminal offence breached Article 8 of the European Convention on Human Rights (ECHR).[27]

---

14 HC Deb 21 Jan 2008 cols 1225–27

15 See for example "Probe into police 'bugging' of MP", BBC News website, 3 February 2008.

16 Report on Two Visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill, Report of Investigation by The Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner, Cm 7336, February 2008.

17 14th Report (2007–08): *Data Protection and Human Rights* (HL 72) (HC 132).

18 22nd Report (2007–08): Government Response to the Committee's Fourteenth Report of Session 2007–08: Data Protection and Human Rights (HL 125) (HC 754).

19 See for example "Council admits spying on family", BBC News website, 10 April 2008.

20 Sir Edmund Burton, Report into the Loss of MOD Personal Data, April 2008.

21 5th Report (2007–08): *A Surveillance Society?* (HC 58).

22 The Government Reply to the Fifth Report from the Home Affairs Committee Session 2007–08 HC 58, A Surveillance Society?, Cm 7449, July 2008.

23 Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008.

24 Kieran Poynter, Review of Information Security at HM Revenue and Customs: Final Report, June 2008.

25 Richard Thomas and Mark Walport, *Data Sharing Review Report*, July 2008, *op. cit.*

26 Ministry of Justice, Response to the Data Sharing Review Report, November 2008.

27 For the text of the judgment see http://www.bailii.org/eu/cases/ECHR/2008/1581.html

A "constitutional approach"

10. The stories that have emerged, and the coverage they have received, have illustrated the importance of the issues which we have been examining. We particularly wish to acknowledge the work of our fellow Parliamentary committees, the House of Commons Home Affairs Committee and the House of Commons Justice Committee, and the Joint Committee on Human Rights, in this field. Whilst we concur with many of their recommendations, we have sought to maintain a distinctive approach to the subject of surveillance throughout the course of our inquiry. In keeping with our remit, we have been especially concerned to focus our attention on the constitutional questions and challenges raised by the spread of surveillance and the practice of data collection. This report seeks to examine surveillance in the context of the UK's constitutional framework, and makes a number of practical recommendations as to how current practices and systems might be improved.

11. We have also sought to identify the constitutional principles that should govern the use of surveillance in the UK today. In the First Report of this Committee, published in July 2001, we observed that the constitution of the United Kingdom is constantly evolving, and that it is embodied in "the set of laws, rules and practices that create the basic institutions of the state, and its component and related parts, and stipulate the powers of those institutions and the relationship between the different institutions and between those institutions and the individual."[28] We also noted that the constitution is founded on five key tenets, namely:

    - The Sovereignty of the Crown in Parliament;
    - The Rule of Law, encompassing the rights of the individual;
    - The Union State;
    - Representative Government; and
    - Membership of the Commonwealth, the European Union, and other international organisations.[29]

12. Central to the success of evolving constitutional democracy has been the British people's commitment to the fundamental principles that underpin these tenets. In particular, there is a widespread belief in the importance of individual freedom and the need for executive accountability and restraint. In the absence of a written constitution which clearly defines the limits of the state and the proper role of government, these principles have continued to inform the relationship between the individual and the state. They have fundamentally shaped the development of our laws, practices, and public institutions.

13. We regard a commitment to the freedom of the individual as paramount. It is a precondition of the functioning of our existing constitutional framework. We also believe that privacy and the principle of restraint in the use of surveillance and data collection powers are central to individual freedom, and should be taken into account and adhered to at all times by the executive,

---

[28] 1st Report (2001–02): Reviewing the Constitution: Terms of Reference and Method of Working (HL 11), paras 18, 20.

[29] ibid., para 21

government agencies, and public bodies. There is a danger that the growing use of surveillance by government and private organisations in the UK could constitute a serious threat to these principles and commitments.

14. Mass surveillance has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country. Central to this inquiry is the question of whether surveillance, which has substantially increased over recent years, represents a threat to these foundations, and to what extent surveillance should be permissible within the current constitutional framework of the UK.

15. In this report, we seek to show how the principles explained above are (or are not) being observed, and how they could be better promoted and protected in the future.

Acknowledgements

16. We have taken a wide range of evidence to inform the report and we would like to thank all those who gave us their views. In the course of this inquiry, we have heard oral evidence from 44 witnesses, and received written evidence from a further 28 witnesses. We have also consulted a large body of secondary evidence, including many of the reports and publications detailed in Box One above. In April 2008, we undertook a visit to Canada and the United States of America, to examine how those nations have managed the issues under consideration.[30] We would like to express our particular thanks to those at the British Embassy in the USA, the British High Commission in Canada, and to all those whom we met on our visit. We would also like to record our thanks to our Specialist Adviser, Professor Charles Raab, Professor Emeritus and Honorary Fellow, University of Edinburgh, and to our Specialist Legal Adviser, Dr Benjamin Goold, Lecturer in Law and Fellow of Somerville College, University of Oxford, for their valuable input and assistance during the course of the inquiry.

[30] A note of the Committee's visit is at Appendix 4.

CHAPTER 2: OVERVIEW OF SURVEILLANCE AND DATA COLLECTION

17. Part One of this chapter explains many of the terms and practices involved in surveillance and the processing of personal data, as well as the principles underlying the current legal and regulatory structure in the UK. Part Two describes the key features of surveillance and the information and communication technology (ICT) that is used by the public and private sectors to monitor individuals. It explains how surveillance and data processing have become prominent features of daily life, focussing primarily on the public sector. Finally, it considers the trends in both the public and the private sectors that arguably pose a challenge to the current system of regulation.

Part One—Key definitions

Background

18. The term "surveillance" is used in different ways. A literal definition of surveillance as "watching over" indicates monitoring the behaviour of persons, objects, or systems. However surveillance is not only a visual process which involves looking at people and things. Surveillance can be undertaken in a wide range of ways involving a variety of technologies. The instruments of surveillance include closed-circuit television (CCTV), the interception of telecommunications ("wiretapping"), covert activities by human agents, heat-seeking and other sensing devices, body scans, technology for tracking movement, and many others.

19. Surveillance and data collection are features of nearly every aspect of the public sector. The processing of personal data has always been part of public administration, and is essential to effective governance and efficient service delivery. But contemporary uses of surveillance and data processing can be distinguished from those of the past in extent and the intensity with which information is analysed, collated, and used. The growing use of CCTV cameras in public and private places, increased reliance on the interception of communications by the police and security services, and the formation of a national scheme of identity cards, are examples of the expansion of surveillance in the UK. Although this inquiry is less concerned with private sector surveillance, we note that activity in this field is widespread and often at the forefront of developments involving advanced surveillance technology and data processing techniques.[31]

20. In 2006 the Surveillance Studies Network produced a report for the Information Commissioner's Office (ICO) which said that "where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance."[32] The collection and processing of information about persons can be used for purposes of influencing their behaviour or providing services.

---

[31] See Lace S (ed.), The Glass Consumer: Life in a Surveillance Society, 2005.

[32] A Report on the Surveillance Society, op. cit., para 3.1.

21. Recent discussions of surveillance have considered the notion that we are living in a "surveillance society". There are a variety of views. In an interview with *The Times* newspaper in 2004 the Information Commissioner, Richard Thomas, expressed his "anxiety that we don't sleepwalk into a surveillance society".[33] The Commissioner told us that surveillance was "traditionally associated with totalitarian regimes but some of the risks can arise within a more democratic framework." (Q 2)

22. Gareth Crossman, the then Director of Policy at Liberty, thought that "now that the language of surveillance society has entered the consciousness, it is useful and appropriate language to use". (Q 221) On the other hand, Mike Bradford, Experian's Director of Regulatory and Consumer Affairs, told us that constant reference to "a surveillance society" only increased public concern, often unnecessarily. (Q 317)

23. Surveillance is rapidly becoming a more intensive and normal instrument of modern government. This was acknowledged by Tony McNulty MP, the then Minister for Security, Counter-terrorism, Crime and Policing at the Home Office, who told us that surveillance is "today's normality. CCTV, DNA database and a whole range of these other elements are not there as a response to exceptional threats and exceptional circumstances … I think that is routine in the 21st century". (Q 927)

Two broad types of surveillance

24. Two broad types of surveillance can be distinguished: mass surveillance and targeted surveillance. Mass surveillance is also known as "passive" or "undirected" surveillance. (JUSTICE, p 109, note 20) It is not targeted on any particular individual but gathers images and information for possible future use. CCTV and databases are examples of mass surveillance.

25. Targeted surveillance is surveillance directed at particular individuals and can involve the use of specific powers by authorised public agencies. Targeted surveillance can be carried out overtly or covertly, and can involve human agents. Under the Regulation of Investigatory Powers Act 2000 (RIPA), targeted covert surveillance is "directed" if it is carried out for a specific investigation or operation. By comparison, if it is carried out on designated premises or on a vehicle, it is "intrusive" surveillance. Targeting methods include the interception of communications, the use of communications "traffic" data, visual surveillance devices, and devices that sense movement, objects or persons.

Uses of personal data

26. The term "surveillance" is sometimes applied to the collection and processing of personal data. The combined term "dataveillance" covers "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".[34] JUSTICE suggested that a common feature of surveillance was "the use of personal data for the purpose of monitoring, policing or regulating individual conduct." (p 109, note 20) Dr David Murakami Wood, Lecturer at the School of Architecture, Planning and Landscape, University of Newcastle

---

33 Ford R, "Beware rise of Big Brother state, warns data watchdog", *op cit*.

34 Clarke R, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, August 2006.

upon Tyne, and representative of the Surveillance Studies Network, said that the use of definitional extremes—which regard all (or at least all unwanted or unjustified) information gathering as surveillance—was unhelpful. He argued that "information gathering with the intent to influence and control aspects of behaviour or activities of individuals or groups would be our working definition." (Q 37)

27. The term "data use" includes those forms of personal data collection and processing relevant to surveillance as defined in the Data Protection Act 1998 (DPA) and the 1995 European Data Protection Directive 95/46/EC (the Directive) that the DPA transposes into UK law. These documents state that the "'processing of personal data' … shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[35]

Data sharing

28. Personal data can be shared in different ways, depending on the technology and information systems used.[36] In the social and health services, for example, data may be placed in a common pool that can be accessed (according to certain rules) by persons either in or connected with the organisation responsible for collecting and storing the information. Data sharing can be conducted between carers, or may follow more complex paths and reciprocal arrangements. The Ministry of Justice told us that data sharing is at the forefront of many state activities in this country. (pp 315–22)

29. Judgments about when and how much data can be shared require difficult decisions. In Chapter 6 we discuss the complex legal and ethical issues which the Government are currently seeking to address. Although the common law and statutory frameworks (such as those established by the Social Security Fraud Act 2001) may provide legal bases for the sharing of data, agency practices and legal uncertainty have inhibited data sharing in the criminal justice system and in some public services. For example, the Bichard Inquiry into the Soham murders highlighted deficiencies in the sharing of information between social services and the police, and recommended an overhaul of procedures, including the provision of better guidance and a code of practice on information practices.[37] The IMPACT programme for information sharing between police forces implements a number of Bichard's recommendations. (National Policing Improvement Agency (NPIA), p 47)

30. The 2008 *Data Sharing Review Report*, by Richard Thomas, the Information Commissioner, and Mark Walport, Director of the Wellcome Trust (the Thomas-Walport Review) states that data sharing of itself is neither good nor bad.[38] The Review opined that the Government's enthusiasm for data sharing has given the impression that they view the practice as an "unconditional good", and that they have paid insufficient heed to

---

35 EU Data Protection Directive 95/46/EC, Article 2(b).

36 Information Commissioner's Office, Framework Code of Practice for Sharing Personal Information, October 2007, p 5.

37 The Bichard Inquiry Report, June 2004 (HC 653).

38 Data Sharing Review Report, op. cit., p i.

corresponding risks and concerns.[39] The Review's recommendations for the better governance of data sharing are considered later in this report.

Data matching

31. Data matching is the technique of comparing different databases so as to identify common features or trends in the data. Matching unemployment benefit claimants against employed persons may, for instance, be a way of identifying potentially fraudulent claimants for further investigation.

32. Similarly, crime scene samples of DNA are frequently matched against the database of DNA samples taken from individuals so as to identify possible suspects. Law enforcement agencies and government have pressed for greater use of data matching to prevent and detect crime, including identity-related fraud.[40]

Data mining and profiling

33. Data mining involves the use of mathematically based analytical tools to detect patterns in large sets of data with the purpose of predicting certain kinds of behaviour, such as the propensity to engage in criminal activity or to purchase particular consumer goods. Profiling is "a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics".[41]

34. In the public sector these techniques may be used, for example, to predict a variety of risk patterns in the population, thereby enabling public services and law enforcement resources to be appropriately focussed. Although this process may enable benefits and social services to be targeted more accurately and effectively, it may arguably lead to discrimination by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions.

35. The use of personal data in data matching and profiling presents challenges to the necessity and proportionality aspects of data protection and human rights legislation. We discuss this further in Chapter 4, paragraphs 122–149.

Privacy

36. There are many definitions and conceptions of privacy.[42] Dr Lee Bygrave, Associate Professor in the Faculty of Law, University of Oslo, took the view that "surveillance, by its very definition, involves a reduction of privacy." However, he argued that it was more difficult to gauge the effect of surveillance on perceptions of freedom, because people can "go around thinking they are free even though they are really in some sort of aquarium." (Q 488) Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), argued that since surveillance was "moving towards a paradigm of preventative measures in which you monitor large groups", the privacy of

---

39 ibid., para 1.10.

40 See for example Home Office, *New Powers Against Organised and Financial Crime*, Cm 6875, 11 July 2006.

41 Clarke R, Profiling: A Hidden Challenge to the Regulation of Data Surveillance, 1993.

42 See for example Schoeman F (ed.), *Philosophical Dimensions of Privacy*: *An Anthology*, 1984; Young J (ed.), *Privacy*, 1978. See also Westin A, *Privacy and Freedom*, 1967; Roessler B, *The Value of Privacy*, 2005.

individuals was inevitably diminished because the courts are only involved in rare cases of complaint or where "an odd thing happens". (Q 505) The loss of privacy in some cases may be harmless and may be offset by the benefits of surveillance and data collection.

37. We consider the issue of privacy in more detail in Chapter 4.

Data protection

38. Data protection laws are often seen as privacy laws by any other name. Many countries have substantially similar laws to our DPA, but call them "privacy" laws and confer the title of "Privacy Commissioner" upon their regulatory official.

39. The system of data protection in the UK is based on the DPA (see Chapter 4), which sets out the laws governing the collection, use and communication of personal data and ensuring the quality of data. In addition, it sets out rules and establishes a regulatory regime for implementing them. "Data protection" is sometimes regarded as a matter mainly of data security—the physical and administrative safeguarding of personal data once it has been collected. This narrow and somewhat technical view, however, does not do justice to the breadth of data protection law as established by the Directive and the DPA. Data protection also involves limiting access to secure data.

Part Two—Characteristics of contemporary surveillance and data use

40. In the rest of this chapter we consider the main features of current surveillance and data use in the UK, and examine how existing practices differ from those of the past.

41. The Surveillance Studies Network identified characteristics of current surveillance practices, including pervasiveness, intensity, speed, interconnection, automation and several others (pp 22–23) on which we report.

The role of technology

42. Surveillance technology is used by governments and private organisations to achieve specific ends, such as maintaining public order, anticipating and meeting social needs, and responding to market trends and consumer demand.

43. The role of technology in surveillance is pre-eminent and poses formidable regulatory problems. The Information Commissioner told us that individuals "leave electronic footprints behind with the click of mouse, making a phone call, paying with a payment card, using 'joined up' government services or just walking down a street where CCTV is in operation. Our transactions are tracked, our interactions identified and our preferences profiled—all with potential to build up an increasingly detailed and intrusive picture of how each of us lives our life. This has increased the capability for surveillance of the citizen through data collection." (p 2)

44. New ICTs enable "ubiquitous computing" or "ambient intelligence" (AmI)[43] to play an increasing role in our lives through the use of embedded devices

---

[43] See Wright D, Gutwirth S, Friedewald M, Vildjiounaite E and Punie Y (eds.), *Safeguards in a World of Ambient Intelligence*, 2008.

which can continuously collect and process information. The devices sense movement and monitor how individuals interact with objects such as vehicles and domestic appliances, making it possible to "customise" the use of technology in the home, the workplace, and elsewhere. New technology, which sometimes incorporates biometric devices such as fingerprint readers or iris scans, can aid in care of the elderly and the infirm, or be used to monitor and control offenders. It is difficult to regulate the effects of AmI where it occurs without people's consent or knowledge.

The impetus behind surveillance and data use

45. Surveillance and data use are becoming increasingly widespread. National security, public safety, the prevention and detection of crime, and the control of borders are among the most powerful forces behind the use of a wide range of surveillance techniques and the collection and analysis of large quantities of personal data.

46. The desire for safety is an example. Councillor Hazel Harding, Leader of Lancashire County Council and Chair of the Local Government Association Safer Communities Board, told us that answers to her Council's questions to residents of Lancashire about issues of importance suggested that "the number one issue for people … is to feel safe. I think it is more than something people aspire to; I think it is a basic human need". (Q 784)

47. The provision of public services of all kinds has become dependent on data collection, sharing, and other related practices. Government activity is dependent on the use of personal data. The economy is fuelled by information processing. Many companies build their businesses around the collection and analysis of data. "Customer-relationship marketing" (CRM)[44] involves "knowing the customer" through intensive surveillance of consumer behaviour.

Large-scale, routine practices

48. Many surveillance practices are now widespread and routine, with data being collected on the entire population and not just on traditional "suspects". The practices are no longer carried out only by specialist bodies such as the police and border control agencies. Information is frequently stored and used as a matter of normal organisational routine. Liberty argued that whilst the proliferation of CCTV has attracted more observation and comment, arguably the most profound societal shift in the last decade has been the growth in the use of mass informational databases. (p 105)

49. The National DNA Database (NDNAD) is rapidly growing, and now contains millions of samples taken from individuals and crime scenes. ContactPoint is intended to be a database that stores data on every child in England and Wales. The National Health Service Care Records Service (NHS CRS), a major part of the computerisation project in the NHS, will include a copy of every patient's medical record. The National Identity Register (NIR) will include information on everyone for the purposes of establishing and verifying their identities. The Government gave us many

---

44 See Evans M, "The Data-Informed Marketing Model and its Social Responsibility", in *The Glass Consumer*, *op. cit.*, Chapter 4, pp 99–132.

further examples of the use and sharing of personal data elsewhere in the public sector. (pp 323–41)

50. Other well-established, extensive databases—such as those authorised by statute for the purposes of taxation, employment, education, benefits, social services, vehicle driving and licensing, and law enforcement—have developed over many decades before and after they were listed and described in the Lindop Report on Data Protection in 1978.[45] Personal data have also been shared across government agencies, and sometimes disclosed to the private sector (for example, employers), without consent.

The availability of technology

51. As ICTs and systems have developed over the years, so has the technology available for monitoring, tracking and identification purposes. Transmitting equipment, in the form of Radio Frequency Identification (RFID) tags, is embedded in industrial and consumer products, physical structures such as buildings, roads, documents, and persons themselves. These enable the movement of goods as well as people to be monitored. The unit cost of hardware and software has fallen dramatically over time, and the collection and storage capacity, functions and versatility of electronic information and communication equipment has expanded. The Royal Academy of Engineering (RAE) has projected the further development of a range of information technology into the foreseeable future.[46]

52. Access to ICTs has long since ceased to be the preserve of large organisations and the wealthy. The means of surveillance and data use are being disseminated throughout most organisations. "Interoperability"—the ability to transfer data easily across a variety of types of equipment—still presents problems, but efforts are being made to overcome them in order to improve co-ordination between organisations and the sharing of data, including personal information.

The global flow of personal data

53. Changes in technology and in the way in which business and government operate mean that information now rapidly flows across national borders, into and out of different sets of legal and other controls, and in ways that are difficult to trace. It is therefore difficult for individuals to hold persons or agencies to account for the processing of personal data.

54. It has proved difficult to establish standardised global rules and practices. This restricts the development of protection against excessive surveillance and data use.

Public sector and private sector data uses

55. The distinction between the public and private sector is becoming increasingly blurred as public services are provided through partnerships and other joint arrangements. Many public sector bodies now employ outside firms to manage their databases. In the public sector, and in joint arrangements, data-based surveillance may be used to assist in the provision

---

[45] Home Office, *Report of the Committee on Data Protection* (Chairman: Sir Norman Lindop), Cm 7341, December 1978.

[46] Dilemmas of Privacy and Surveillance: Challenges of Technological Change, op. cit., Chapter 3.

of social benefits to individuals or groups, and in the identification of people who may be either at risk of harm or who pose a risk to others if they are not identified and properly treated. The Government provided information on the many circumstances in which personal information is, or will be, gathered and used by the public sector. (pp 323–41)

56. The development of "e-government" and "Transformational Government",[47] including the sharing of personal data across departments and agencies, represents a major innovation in the UK public sector. What is sometimes called the "database state" (NO2ID, pp 424–26) is the object of public attention when there are breaches of security and data losses, theft or expenditure overruns.

57. The Government drew attention to the relationship between central and local government, for example in respect of the advice and guidance given by the Department of Communities and Local Government (CLG) to local authorities on the use and sharing of personal information in their revenues and benefits departments. (pp 323–41) Local authorities are some of the most frequent users of personal information. They are also among those bodies which are permitted to conduct surveillance operations under RIPA,[48] and they deploy and control most public-space CCTV systems.

58. Private sector surveillance is prevalent in the majority of commercial environments, such as shopping centres, supermarkets, stores, and banks. It has also become an inescapable aspect of life on the internet, where the browsing behaviour of online shoppers is routinely recorded and analysed by companies and marketing firms. Surveillance now plays a major role in the workplace, with many employers monitoring the behaviour of employees in order to assess performance and prevent the use of online facilities for private purposes.[49]

59. There are many other instances of private sector surveillance. The technology contained in mobile telephones makes it possible for companies to monitor communications and track geographic location. Camera systems can be used to watch over warehouses, industrial and business premises that cannot be patrolled easily or cheaply using guards. Domestic surveillance devices can be readily purchased and installed in private residences.

60. The widespread use in CRM of consumer databases, which are matched, mined, shared, rented, and sold commercially, has become a central feature of business activity. Trevor Bedeman, an independent consultant specialising in data and information sharing, drew attention to data sharing practices within the private sector. (p 385)

61. Credit referencing activities depend on the processing of personal data, which is also indispensable for combating financial fraud. Mike Bradford told us of Experian's concern to maintain the trust of business clients and the public in the way in which they safeguard and use personal data. (QQ 346, 350)

62. On the other hand, Toby Stevens, Director of the Enterprise Privacy Group, told us that, although private companies are obliged to comply with data protection principles, human rights and related laws, there is no duty to offer

---

47 Cabinet Office, Transformational Government—Enabled by Technology, Cm 6683, November 2005; Information Sharing Vision Statement, op. cit.

48 See paragraphs 164–178.

49 Carvel J, "Most employers restrict staff time on internet, says survey", *The Guardian*, 2 December 2008.

privacy. He argued that "privacy is, in fact, a secondary benefit to the consumer arising from good commercial practice". (Q 343)

63. The RAE argued that schemes such as Oyster cards and store loyalty cards "effectively collect data about peoples' journeys and purchases by stealth, as the user may be unaware that such information is generated when they are used. It is not obvious that a loyalty card designed to attract customers into a store will be used to harvest personal information used in marketing, and it is not clear that the card should have to function in that way." (p 435)

64. Mike Bradford told us that Experian were actively working with government on how public and private sector data can come together. (Q 362) The Government have also been exploring ways of exchanging data with the private sector to combat financial fraud through membership of CIFAS, the UK's Fraud Prevention Service.[50]

65. The Information Commissioner thought it was not surprising that the police, the security services and other agencies wanted access to private sector databases, but he alluded to the dangers of a "free for all":

> "It is a fundamental principle of data protection that information collected for one purpose should not be used for another unless certain requirements are met. So we are not saying that there should never be access to private sector databases, but we are saying that it should be controlled." (Q 18)

66. The trend towards more data sharing suggests that the difficulty of tracing what happens to personal data, and of maintaining clear lines of accountability and responsibility for them, will increase over time, with implications for the current regime of regulatory safeguards for the citizen.

67. In the following chapters, we consider these issues in detail and offer recommendations on safeguards against intrusions on privacy and excessive surveillance.

---

[50] Home Office, New Powers Against Organised and Financial Crime, Cm 6875, July 2006.

CHAPTER 3: ADVANTAGES AND DISADVANTAGES OF SURVEILLANCE AND THE USE OF PERSONAL DATA

68. The Government told us that:

> "There is a need to gather and access personal information to: support the delivery of personalised and better public services; fight crime and protect public security; reduce the burden on business and the citizen, and tackle social exclusion through early intervention. This processing of personal information is demanded in greater quantity and in quicker time than ever before". (p 316)

69. The Government's evidence does not of itself explain how the collection of information helps the pursuit of their objectives, or whether existing processing practices are proportionate to those objectives. Surveillance and the use of personal information may lead to a conflict between the interests of the citizen and the goals of the state, and the gathering of personal information has the potential to undermine privacy and limit the freedom of the individual. In this chapter, we consider the advantages and disadvantages of surveillance and the use of personal data in two areas: law enforcement and public safety; and the provision of public services.

Advantages of surveillance and the collection of personal data—Law enforcement and public safety

CCTV

70. Protecting the public is a duty of government. According to the Surveillance Studies Network, during the 1990s approximately 78 per cent of the Home Office crime prevention budget was spent on installing CCTV, whilst some £500 million of public money was invested in CCTV in the decade up to 2006.[51] Where previously this money might have been spent on street lighting and supporting neighbourhood crime prevention initiatives, it is now used to maintain and expand the network of police and local authority cameras. It is difficult to determine exactly how many CCTV cameras there are in the UK (Q 44) but recent estimates have put the figure at over 4 million.[52] Most experts appear to agree that the UK leads the world in its use of CCTV.

71. A number of witnesses referred to public attitudes to CCTV. Councillor Hazel Harding, Leader of Lancashire County Council and Chair of the Local Government Association Safer Communities Board, told us that:

> "CCTV is very popular with law-abiding members of the public who see it as a preventative and feel much safer … CCTV is something that councils are facing demands for day after day from members of the public who think it would actually make them safe and they would feel safer because of it." (Q 771)

72. We consider public attitudes towards CCTV in more detail in Chapter 8.

73. A number of witnesses referred to the benefits of CCTV. Hazel Harding told us that:

---

51 A Report on the Surveillance Society, op. cit., para 9.5.3.

52 ibid., para 9.5.2

> "There are some good examples of how CCTV has helped perhaps not always to prevent but certainly to detect crime and as such it has been very useful … In terms of antisocial behaviour, I do not think necessarily that people out on the streets sometimes causing mayhem look at where the cameras are or behave differently because of it, but I do think that it does enable prosecutions and, as such, is very useful." (Q 771)

74. The Association of Chief Police Officers (ACPO) agreed that "the availability of CCTV images greatly assists in the investigation of crime and disorder", although they added that "the contribution of CCTV images … is not recorded in a systematic manner". (p 43) ACPO gave examples of CCTV's effective use in terrorist trials, tracking suspicious vehicles along with number-plate recognition, and suspicious behaviour in a town centre. (pp 43–44)

75. Deputy Chief Constable Graeme Gerrard of the Cheshire Constabulary and Chair of ACPO's CCTV Working Group said:

> "When a crime has occurred CCTV is a vital element of the investigative process. It is not an understatement to say now that the first piece of evidence that an investigating officer will go looking for is the CCTV evidence. The first investigative action very often is [to] secure all available CCTV evidence … You only need to watch the television on a daily basis and to read the media on a daily basis to see how many crimes are detected, or certainly the investigation greatly assisted, as a result of CCTV evidence." (Q 146)

76. He also said:

> "Several years ago London was suffering from a nail bombing campaign by an individual … targeting specific parts of London with his nail bombs and there were extremist groups claiming responsibility for the actions. That event was entirely supported by CCTV evidence in terms of actually detecting that crime. What value do you put on the price of that detection?" (Q 148)

77. Transport for London (TfL), which uses some 10,000 CCTV cameras in its rail network, stations, roads and buses, argued that:

> "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 … 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 … CCTV coverage … remains an essential component of protecting the system from terrorism and providing essential intelligence to the Police and security services". (pp 340–41)

78. Graeme Gerrard acknowledged that the use of CCTV has limits:

> "The evidence and academic research that I have seen says it is very effective in places like car parks … but in terms of our town centres, where a lot of the behaviour is violent or disorderly … often fuelled by alcohol, people are not thinking rationally, they get angry and the CCTV camera is the last thing they think about and even the presence of police officers does not deter them … In terms of reducing crime there are mixed results … there was some quite good indication that it reduces the public's fear of crime. If you look at where most of the pressure is for

> CCTV in the community, the vast majority of it comes from the public who actually want it … It is certainly not being driven by the Police Service, it is actually being driven by the local communities." (Q 145)

79. Professor Clive Norris, Professor of Sociology and Deputy Director of the Centre for Criminological Research at the University of Sheffield, and representative of the Surveillance Studies Network, referred to research that showed that improved street lighting "seemed to be a rather more effective form of prevention" than CCTV. (Q 40) Professor Martyn Thomas, independent consultant and representative of the UK Computing Research Committee (UKCRC), and Dr Ian Forbes, Director of fig one Consultancy, and representative of the Royal Academy of Engineering (RAE), also drew attention to several factors that contribute to crime deterrence. (Q 394) Professor Janice Morphet, a former local authority officer and Chief Executive, thought "it would be more worthwhile to have a more integrated approach to thinking about on-street safety, which would include design, CCTV, and the presence of police and other officials." (Q 913)

80. In an effort to improve the effectiveness of CCTV, the Home Office and ACPO have developed a national strategy to overcome technical, organisational and human problems.[53] Whilst noting the usefulness of research into the prevention and deterrent effects of CCTV, the Home Office and ACPO said that "little formal research has been undertaken to establish the impact that CCTV has on the investigation of crime. Those examining the issue therefore have to rely on limited research and anecdotal evidence provided by operational police officers."[54]

81. The House of Commons Home Affairs Committee's report recommended that "the Home Office undertake further research to evaluate the effectiveness of camera surveillance as a deterrent to crime before allocating funds or embarking on any major new initiative. The Home Office should ensure that any extension of the use of camera surveillance is justified by evidence of its effectiveness for its intended purpose, and that its function and operation are understood by the public."[55] The Government's response stated that this recommendation was "being addressed through the National CCTV Strategy."[56] There is no reference to the substance of the Home Affairs Committee's recommendation in the strategy document.

82. **We recommend that the Home Office commission an independent appraisal of the existing research evidence on the effectiveness of CCTV in preventing, detecting and investigating crime.**

83. We consider later in the Report how CCTV should be regulated (see paragraphs 213–19).

DNA

84. Personal data in the form of DNA are routinely collected from individuals and crime scenes by the police. Since the establishment of the National DNA Database (NDNAD) in 1995, DNA profiling has increased, with law enforcement agencies using DNA and other forms of "bioinformation" for

---

53 National CCTV Strategy, op. cit. October 2007.

54 ibid., section 5.1.

55 *A Surveillance Society?*, op. cit., para 222.

56 The Government Reply to A Surveillance Society?, op. cit., p 15.

crime detection, to assist in the investigation and prosecution of criminals, and to help identify deceased persons and body parts. A number of witnesses referred to the advantages of the forensic use of DNA data. We consider this evidence, in the context of the issues associated with DNA collection and profiling, in Chapter 4.

Covert surveillance

85. Covert surveillance includes the undisclosed tracking of individuals, interception of the contents of communications, the analysis of "traffic data"—the record of, for example, who telephoned whom and when—and the use of human agents in undercover activities.

86. Assistant Chief Constable Nick Gargan, the former Chair of the Covert Investigation (Legislation and Guidance) Peer Review Group within ACPO told us that "the use of covert surveillance is indispensable to the Police Service and to our colleagues involved in the fight against all forms of criminality … citizens are very happy to support the development of surveillance and of data acquisition mechanisms that achieve a balance between privacy and safety." (Q 90)

Combating fraud

87. Combating fraud is a law enforcement activity which uses data collection and processing. Evidence from the Government's Fraud Review described a policy development to combat fraud, which would include extensive information sharing and the linkage of databases. Success is already claimed in respect of NHS savings of £189 million in 2005, the National Fraud Initiative's savings of £111 million in 2005–06, and £10 million saved in respect of cheque and plastic card fraud. (p 329)

88. The Department for Business, Enterprise and Regulatory Reform (BERR) is authorised to carry out covert or other non-intrusive forms of surveillance. It regards these powers and methods as "fundamental, basic and crucial utensils of any investigative toolbox" in pursuit of, for example, company and insolvency fraud, and suspected fraud of health-related compensation schemes. (pp 324–26) The Department for Work and Pensions (DWP) gathers personal data from a range of other departments and local authorities, in part "to prevent and detect fraudulent claims, for example by matching death information from the General Register Office with our customer records". (p 340) Benefit fraud control at the local authority level also involves the matching of personal data files. Professor Morphet described how recent improvements in IT systems had led to data matching being used to identify people committing benefit fraud. (Q 887)

Advantages of surveillance and the collection of personal data—Provision of public services

89. For the citizen, the potential of being able to obtain public services from central or local government quickly, reliably, and efficiently is justification for electronic government ("e-government"). Through the electronic co-ordination of health and social care, public transport, education and children's services, and recreational facilities, e-government aims to improve the delivery of public services by, for example, providing faster diagnosis and treatment, the monitoring of personal performance and progress, easier

payment systems and bookings, and the online provision of targeted information.

90. The Prime Minister has advocated the advantages of bringing information together to serve citizens better:

> "By sharing information across the public sector—responsibly, transparently but also swiftly—we can now deliver personalised services for millions of people, something not dreamt of in 1945 and not possible even ten years ago. So for a pensioner, for example, this might mean dealing with issues about their pension, meals on wheels and a handrail at home together in one phone call or visit, even though the data about those services is held by different bits of the public and voluntary sectors."[57]

91. Better information management means that citizens can carry out transactions with the state for claiming benefits, paying taxes, applying for licences, registering and revising basic information, and for other purposes through a single window or gateway, either online or in government offices, avoiding the need to provide the same information many times over to separate government departments. Michael Wills MP, Minister of State in the Department of Justice with responsibility for data handling issues, said:

> "We know for example that there is a big problem with the take up of free school meals and a lot of young children are not getting adequate nutrition … The information that would enable us to identify those young children is available to us … That is a good that everybody can subscribe to but it does depend on data sharing to improve that level of take up. Similarly Sir David Varney[58] when he was looking at this quotes an example of a bereaved family who had lost a family member in a road accident. In these tragic circumstances the last thing you want to do is to be badgered with lots of information. I think they had 44 different contacts with the state in different ways and that is unacceptable. These things need to be done but if you could share the data the level of intrusion into a family in grief is minimised." (Q 975)

92. Through the intensive analysis of large collections of personal data, it is now possible for government to be more "citizen-focussed" and for services to be better tailored to individual needs and circumstances. Professor Morphet told us:

> "Many citizens are not actually receiving their full entitlements. There are just over 50 different kinds of financial benefit that a citizen could be entitled to, and … 80 per cent of the information required for those applications for benefit was the same. The current system would be that a citizen would have to fill in as many forms for these benefits as they thought they were entitled to, but a modernised local government approach would suggest that you collect the information once and, with the citizen's consent, you see if they are entitled to other benefits." (Q 883)

93. Professor Morphet gave an illustration of how data comparisons across local agencies are used to identify families suffering from a range of related

---

57 Gordon Brown MP, Speech on Liberty, op. cit.

58 Sir David Varney, Service Transformation: A Better Service for Citizens and Businesses, a Better Deal for the Taxpayer, December 2006.

problems, and to ensure that any new initiatives aimed at helping them are accurately targeted:

> "I am thinking of the case of one particular council … that identified that certain families had a cluster of problems when they looked at issues, and compared some information across agencies. These families were clustered on an estate, and there were high levels of truancy, crime, debt, poor health and so on … [The council] have been in and targeted that area for a range of initiatives to improve the situation." (Q 900)

94. The Department of Communities and Local Government (CLG) outlined benefits of social service information-sharing to the citizen in terms of better assessment of clients' needs and the effective tailoring of services. In addition it claimed that information sharing can help in the design of services and the monitoring of their performance and effectiveness. (pp 326–29) The Department for Children, Schools and Families (DCSF) stated that:

> "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." (p 330)

95. Evidence on the advantages of data collection and sharing that we received from some central government departments via the Ministry of Justice constituted policy aspirations with little comment on outcomes. (pp 323–41)

Data collection and public policy formation

96. The collection and processing of data on sections of the population is important to the development of future public policies. Predictive and proactive strategies based on the analysis of personal data are, controversially, becoming more important in relation to the provision of children's services. Dr Eileen Munro, Reader in Social Policy, London School of Economics (LSE), told us that the desire "to monitor and ensure all children are reaching some standard of experience is very recent." (Q 813)

97. Dr Christopher Hall and his colleagues in the e-Assessment in Child Welfare research project, University of Huddersfield, explained:

> "Social policy commentators have observed the expansion of state intervention with children. 'Every Child Matters'[59] heralds a more universal view, focusing on 'children with additional needs', rather than children 'at risk' or 'in need', as in earlier legislation. The Government aims to identify and track around a third of children who require interventions beyond universal services." (p 398)

98. These programmes of Transformational Government emphasise the importance of sharing information contained in different departmental or agency "silos", using technology to enable better and novel forms of service provision, and the delivery of more effective policy outcomes.[60] We discuss this more fully in Chapter 6.

---

59 Department for Education and Skills, *Every Child Matters*, Cm 5860, September 2003.

60 Transformational Government—Enabled by Technology, op. cit.; Information Sharing Vision Statement, op. cit.

Disadvantages of surveillance and the collection of personal data

99. Our attention was also drawn to the potential costs and dangers of surveillance and the collection of personal data. As we have already noted, the Information Commissioner, Richard Thomas, has stated that there is a danger that Britain is sleepwalking into a "surveillance society", in which the tools of mass surveillance have become ubiquitous and individual privacy a thing of the past.[61] Although none of the witnesses we heard from went so far as to suggest that we are living in an Orwellian society—or that one is just around the corner—many endorsed the Commissioner's concerns and argued that the steady expansion in the surveillance apparatus of the state and private sector had already transformed the everyday lives of millions of people, and not always for the better. Privacy, trust in the state, and the security of our personal information were all now at risk owing to the growth in surveillance, and there was a pressing need to take the potential pitfalls of surveillance seriously. (Professor Norris, Q 54; Professor Graham Greenleaf, Q 77; Professor Peter Hutton, Q 169)

The threat to privacy and social relationships

100. In the opinion of many of our witnesses, the widespread use of surveillance technology poses a significant threat to personal privacy and individual freedom. Liberty argued that the shift towards mass surveillance technology has the potential to affect large sections of the public, and to render privacy, and the personal autonomy that flows from it, vulnerable: "It is not only those that have something to hide that have something to fear, something to protect." (p 103)

101. This point was also made by Professor Ian Loader, Director of the Centre for Criminology, University of Oxford, who drew particular attention to the threat to privacy from state surveillance:

> "Privacy must and should remain an important part of our conversation when we think about surveillance … because the capacity to control information about your life … seems to me an important part of what it means to have … a sphere of autonomy within which to operate that the state cannot encroach upon." (Q 631)

102. The widespread use of surveillance may undermine the value of privacy as a public good. JUSTICE argued that it is important to recognise the public dimension of privacy, and to acknowledge its role in the development and operation of a range of social relationships. (p 109)

103. **As surveillance is potentially a threat to privacy, we recommend that before public or private sector organisations adopt any new surveillance or personal data processing system, they should first consider the likely effect on individual privacy.**

Surveillance and trust in the State

104. We took note of evidence that the growing spread of surveillance was slowly transforming our constitutional landscape. Although there is nothing inherently unconstitutional in the use of surveillance by the state, there is nonetheless a danger that it may disturb some of the presumptions and

---

[61] See paragraph 2.

relationships that underpin the relationship between the individual and the state. As Dr David Murakami Wood, Lecturer at the School of Architecture, Planning and Landscape, University of Newcastle upon Tyne, and representative of the Surveillance Studies Network, observed:

> "We exist in a society of a kind of tacit social contract where we expect to be free and to have those freedoms protected and the main reason for security is to protect our rights to go about our daily business unhindered. Where that protection starts to remove those freedoms themselves, I think that tacit contract is challenged". (Q 64)

105. Many witnesses suggested that surveillance changes the nature of the relationship between the individual and the state. According to NO2ID, our legal system is based on direct relationships between individuals and institutions, with legal rules being aimed at answering the question, "Does this person have this right in these circumstances?" However, they argued, as a result of increasing levels of routine surveillance, and particularly database surveillance, "the growing culture of state identification and record keeping is eroding that fundamental assumption of law." (p 426)

106. NO2ID suggested that increased emphasis on records and centralised databases undermines the presumption of innocence by making anyone who is not willing to provide requested information to government a target of suspicion. They also argued that the growing expectation that individuals are responsible for ensuring that their data are up to date creates a new and increasingly onerous set of personal obligations:

> "The idea of continuous self-exculpation is aligned with the pragmatic consequence of surveillance mechanisms. The records must be complete. Therefore they must be kept up to date. Therefore the citizen acquires new and onerous obligations backed by penalties for non-compliance, to report on himself." (p 428)

107. Professor Norris agreed that by placing increasing emphasis on surveillance and the collection of data, government was sending a clear message to members of the public:

> "Mass surveillance promotes the view … that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted". (Q 54)

108. We also heard evidence that loss of trust in the state could have serious consequences for the functioning of government. In many instances, trust in the state is an essential prerequisite for compliance with the law, and as a result anything that undermines trust has the potential to generate resistance and lead to the creation of an antagonistic relationship between the individual and the state. According to Dawn Oliver, Emeritus Professor of Constitutional Law, University College London:

> "For me a major problem is the risk that individuals will feel that they cannot trust the state with the information that it has about them and that might make them feel insecure and unwilling to co-operate with the state, unwilling to provide information … because they are concerned it might be either lost or get into hands they do not want the information to get into. For me the main thing is this question of security, trust and co-operation." (Q 742)

109. In similar vein, Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), suggested that the growing use of surveillance technology by the Government and the expansion in investigatory powers was part of a "battle of arms between police and criminals with technology as a primary instrument." One consequence is that the citizen is subject to increasing levels of surveillance. (p 172)

110. **Before introducing any new surveillance measure, the Government should endeavour to establish its likely effect on public trust and the consequences for public compliance. This task could be undertaken by an independent review body or non-governmental organisation, possibly in conjunction with the Information Commissioner's Office.**

Surveillance and discrimination

111. We also took evidence about the social effects of surveillance. The Information Commissioner's Office (ICO) drew attention to the potential for discrimination. The ICO focussed on plans by the Government to identify and monitor children:

> "Moves are already underway to try to identify children who may grow up into one of the 20% of adults who are believed to commit 80% of the crime. This involves analysing circumstantial risk factors such as family members' criminal records. This runs the real risk that children are stigmatised from an early age and however well behaved they may be are treated with suspicion." (p 3)

112. The Information Commissioner argued that "the more you use profiling the more you run the risk of … greater stigmatisation, more discrimination, more social exclusion and a society of greater suspicion where trust is reduced." (Q 4) Professor Norris suggested that surveillance encourages discrimination because it leads to the Government and private organisations shifting their focus from a concern for the individual to a desire to categorise and manage populations. (QQ 54, 55) He added:

> "[The] problem is that once you are into a surveillance solution, it becomes in a sense expansionary to a huge degree. If you see that information is what you need to solve a problem but you do not quite know what that problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people". (Q 54)

113. Professor Norris contended that existing surveillance systems and databases may reflect long-standing institutional biases and provide a basis for discrimination based on factors such as race:

> "The over-representation of black men in the DNA Register is a serious issue and cause for concern and part of that over-representation is because they are more likely to be arrested by the police … So, we have a system that is disproportionately including someone on a register which will affect their life chances in ways in the future which is based on forms of differentiation". (Q 55)

Surveillance and personal security

114. The amount of personal information held by the state and the private sector is of concern because of its potential implications for personal security. A number of witnesses noted that the potential consequences of data loss or misuse have grown. As we noted in Box One, over the past two years, a succession of data losses by various government agencies have occurred. The UKCRC said that:

> "No collection of data is 100% secure. There is a growing list of mistakes and unintended outcomes, which have implications for individual citizens' liberty, privacy and life chances. When this happens, individuals usually find it difficult to put the record straight, or obtain compensation or redress." (p 147)

115. The routine collection and storage of personal data makes individuals vulnerable to criminal organisations stealing and misusing their information. The ICO told us that there is a "thriving black market in personal details" and that the accidental loss of personal data by government and private organisations puts individuals at serious risk of identity fraud. (p 3)

116. The UKCRC made specific recommendations to improve data security, and thus reduce the risks associated with growing levels of state and private surveillance. They suggested that organisations that are legally required to retain personal data should be required to encrypt the data so as to prevent unauthorised access and mitigate the effects of any loss. (p 147)

117. **We welcome the UK Computing Research Committee's suggestion that the encryption of personal data should be mandatory in some circumstances. Organisations should avoid connecting to the internet computers which contain large amounts of personal information. We recommend that the Government introduce appropriate regulations.**

CHAPTER 4: LEGAL REGULATION AND SAFEGUARDS

118. The regulation of surveillance and data use is provided by statutory rules, common law decisions, and Codes of Practice and guidelines issued by regulatory authorities and by public and private organisations. Evidence focused on four main sources of domestic regulation:

- The Human Rights Act 1998 (HRA);
- The Data Protection Act 1998 (DPA);
- The Regulation of Investigatory Powers Act 2000 (RIPA); and
- The tort of breach of confidence.

119. The Ministry of Justice argued that the current legal framework is "responsive and robust enough to meet both current and future needs." (p 315) While acknowledging that the pace of technological change presented challenges to the Government, Tony McNulty MP, the then Home Office Minister for Security, Counter-terrorism, Crime and Policing, expressed the belief that the fundamentals of the regulatory system were sound, and that the boundaries between acceptable and unacceptable surveillance were "very, very clear". (Q 936, 942)

120. Dr David Murakami Wood, Lecturer at the School of Architecture, Planning and Landscape, University of Newcastle upon Tyne, and representative of the Surveillance Studies Network, suggested that an incremental approach to the development of regulations and safeguards could not keep pace with the speed of technological change and that, unless a greater effort was made to harmonise the various parts of the present legal framework, the Government would be poorly placed to respond effectively to future developments in the field of surveillance and data use:

> "We need to move ahead of the game ... The first thing to do is bring together those existing pieces of legislation, start to connect them, start to see where the holes are, to fill those holes and … to actually start to think in terms of the future about what might occur and how we might legislate for things that are now being developed or will be developed." (Q 67)

121. In this chapter, we look at the various sources of regulation, and consider how effective they are at controlling the surveillance activities of the state and the private sector. We also look at how effectively two major forms of surveillance and data collection, the National DNA Database (NDNAD) and CCTV, are regulated.

The Human Rights Act 1998

122. David Feldman, Rouse Ball Professor of English Law, University of Cambridge, argued that prior to the enactment of the Human Rights Act 1998 (HRA), there was no established right to privacy in UK law. (Q 522) Although individuals could appeal to the European Court of Human Rights if they felt that their right to privacy under Article 8 of the European Convention on Human Rights (ECHR) had been infringed, the right could not be pleaded in UK domestic courts. With the introduction of the HRA, however, the ECHR became a part of domestic law, and a general right to respect for private and family life under Article 8 was established in the UK.

As a consequence, it became unlawful for any public body to act so as to interfere with an individual's privacy unless the body could point to one of the specific exceptions contained in Article 8(2). Although under the HRA the provisions of Article 8 can only be enforced against public bodies, in recent years the UK courts have sought to expand its ambit so that it can, under certain circumstances,[62] also be applied to private bodies and individuals. The courts have also taken decisions extending the common law tort for breach of confidence in the field of individual privacy interests. (Dr Metcalfe, Q 244)

123. Article 8 of the ECHR provides the basis for a general right to respect for privacy and family life, but there is no accepted legal definition of privacy. Privacy is difficult to define, and both the European Court of Human Rights and UK courts have declined to offer a definition, preferring to judge the right on a case by case basis. While the European Court of Human Rights has not produced a definition of privacy as such, we note that it has been clear in stating that Article 8 encompasses a right to establish and develop relationships with other human beings.

124. The definition of privacy given by Samuel Warren and the future US Supreme Court Justice Louis Brandeis in 1890, which held that an individual has the "right to be let alone", is perhaps too brief and concise to cover the range of circumstances and concerns considered in this report.[63] In 1990 the Calcutt Committee on Privacy and Related Matters adopted a helpful definition in its first report on privacy:

> "The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information."[64]

125. The incorporation of Article 8 into UK law via the HRA means a public body engaged in any form of interference with an individual's privacy must be able to demonstrate that the surveillance in question is:

    (i) authorised by law;

    (ii) proportionate to the purpose in question;

    (iii) necessary; and

    (iv) conducted in accordance with one of the legitimate aims set out in Article 8(2) of the ECHR.

126. The HRA and Article 8 of the Convention provide a privacy-based framework for the regulation of surveillance and data use in the UK. According to many of our witnesses the introduction of the HRA has led to a positive change in the way in which government agencies and private organisations approach matters of surveillance and data use. (Dr Metcalfe, Q 244; Professor Feldman, Q 525) We were told, for example, by Dr Eric Metcalfe, Human Rights Policy Director for JUSTICE, that Article 8 provides a basis for the development of a right to privacy in the UK, and that it has the potential to transform the way in which surveillance and privacy are handled. (QQ 244, 247)

---

62 See, for example, the decision in *Campbell v Mirror Group Newspapers* [2004] UKHL 22.

63 Warren, S. and Brandeis, L. (1890), "The Right to Privacy", *Harvard Law Review*, 4(1), pp 193–220.

64 Report of the Committee on Privacy and Related Matters (Chairman David Calcutt QC), Cm 1102, 1990, p 7.

127. The incorporation of Article 8 into domestic law has affected the common law action for breach of confidence, which has historically acted as the primary protection for privacy interests in the common law. (Hugh Tomlinson, pp 439–40) According to Dr Metcalfe:

> "It has been interesting, since the Human Rights Act, in particular, to see the development of the common law in this area … We find the courts are now beginning to develop the traditional common law breach of confidence principles and use that to act as a more general remedy for breaches of a person's Convention rights since the Human Rights Act came into force." (Q 244)

128. A number of witnesses drew attention to the limitations of the HRA and Article 8 of the Convention. According to Article 8(2) an interference with the right is permissible "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 noted by Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), in practice governments can interpret these limitations freely, without having to point to any empirical evidence about the need for such a limitation. (Q 492)

129. Concerns were also raised about whether government agencies and other public bodies understand how the principles of necessity and proportionality operate in the context of privacy and the limitations set out in Article 8(2). In order to justify an interference with the Article 8 rights, on the basis of any of the exceptions laid out in Article 8(2), the state must be able to show that it is acting lawfully and for a legitimate aim, and that the interference is both necessary and proportionate. (Hugh Tomlinson, p 440) As Professor Feldman pointed out, the proportionality test can be "a very effective protection indeed". (Q 520)

130. We were told that neither the European Court of Human Rights nor the English courts have applied a rigorous proportionality test in the context of interferences with Article 8. According to Hugh Tomlinson:

> "The crucial question is always that of proportionality … If the grounds on which it was justifiable to interfere with the right to privacy were to be restricted this should be done by requiring a stricter proportionality test to be satisfied." (p 440)

131. We took evidence from a number of witnesses about the manner in which Article 8 rights have been pursued in the courts, and the extent to which they have provided a defence for the privacy interests of citizens. According to Dr Chris Pounder, then of Pinsent Masons:

> "I am not confident that Article 8 will provide satisfactory jurisprudence because there are very few cases going to the courts. Those cases that tend to go into the courts primarily involve … people who have celebrity status … Anybody who is trying to take an Article 8 case on has to take on the unlimited resources of the state." (Q 842)

132. While the introduction of the HRA has helped to ensure that the privacy of citizens is better protected, we are concerned that Article 8 is not well understood by the public. The protections offered by the HRA against

unlawful and overly intrusive surveillance are not readily accessible or comprehensible to most members of the public.

133. Although the rights contained in Article 8 provide a substantial measure of privacy protection for the public, the law in this area is developing slowly. JUSTICE suggested that there has been a tendency on the part of the Government and the courts to see Article 8 as providing a minimum standard that must be attained rather than as a foundation for the development of better regulation. (p 110) We believe that more should be done to ensure that the HRA acts as a sufficient brake on intrusive surveillance practices and over-zealous data collection.

134. In the light of these concerns, **we recommend that the Government should instruct government agencies and private organisations involved in surveillance and data use on how the rights contained in Article 8 of the European Convention on Human Rights are to be implemented. The Government should provide clear and publicly available guidance as to the legal meanings of necessity and proportionality. We recommend that a complaints procedure be established by the Government and that, where appropriate, legal aid should be made available for Article 8 claims.**

135. Evidence was taken on the effectiveness of Article 8 in respect of loss of privacy. The spread of surveillance technology has the potential to affect large numbers of people in many ways. Gareth Crossman, the then Director of Policy at Liberty, argued that for a human rights based approach to privacy to work effectively, there is a need for a victim to bring an action. As a great deal of surveillance—particularly mass informational surveillance—affects "a very large number of people, but only in small ways", singling out a particular victim or identifying a single, serious harm may be extremely difficult. (Q 244)

136. The introduction of the HRA has helped to ensure that the privacy of citizens is better protected, but the right to privacy alone cannot provide an adequate basis for the protection of individuals against over-zealous surveillance or data processing. There should be greater support given to groups who may have seen their overall privacy diminished by mass surveillance or the adoption of new data collection and sharing techniques by government.

137. **The Government should consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government and private surveillance practices on the rights of the public at large under Article 8 of the European Convention on Human Rights.**

138. The primary aim of this inquiry was to consider the constitutional implications of surveillance and data use, including the question of whether citizens have a constitutional expectation or right to privacy. There was a range of views on the question of whether the rights contained in Article 8 have the status of constitutional principles or rights. Hugh Tomlinson did not think "that there are any specific constitutional conventions or principles directly relating to surveillance or data protection." He explained that:

> "The major legal obstacle to the better protection of privacy in the United Kingdom is the absence of a strong 'constitutional' privacy right. Although the Courts have, in response to the impetus provided by the Human Rights Act 1998 developed a wide range of 'constitutional

common law rights' in other areas, privacy has not been so recognised and Article 8 has, at present, only partially filled the gap." (pp 439–40)

139. Professor Feldman told us that, whilst he was "not entirely convinced that surveillance generally raises important constitutional issues of an institutional kind", he did think that a number of "constitutional principles" might come into play when considering the proper limits of state surveillance. (QQ 517–18) In particular, he drew attention to the clear constitutional requirement that ministers are accountable to Parliament, and suggested that any surveillance or data collection activities undertaken under the authorisation of a minister should be open to parliamentary scrutiny. He added:

> "The UK's constitution has long relied on what one might describe as a principle of executive and legislative self-restraint in interfering with people or authorising interference with people and their activities. That is an important principle, although it is very rarely written about in any of the text books, and it is important because of the centrality of the idea of the legislative supremacy of the Queen in Parliament. If you have a situation in which the Queen in Parliament can authorise in principle anything, then it becomes very important to be self-controlled in the way in which those powers are used, so I like to think that there is a principle of both executive and legislative self-restraint that is increasingly under strain, I think, at the moment." (Q 518)

140. We heard evidence about the constitutional implications of surveillance and data use from a number of civil liberties and human rights organisations. JUSTICE stated that it "regard[s] the Human Rights Act 1998 as a constitutional document and the rights protected therein as constitutional rights" (p 110), and drew our attention to a recent lecture by Lord Steyn, in which he argued that:

> "[A] premise of the democratic idea is that the basic values of liberty and justice for all and respect for human rights and fundamental freedoms are guaranteed. It is enshrined in the Human Rights Act 1998 which is our Bill of Rights".[65]

141. But JUSTICE also stated that it is "important to bear in mind the limitations of the constitutional framework for the protection of constitutional rights in the UK", and that:

> "It is a mistake to suppose that judicial supervision is enough to maintain privacy as a public good in the UK. In particular, Parliament cannot abdicate to the courts its responsibility to govern well, in particular by restraining the executive's enthusiasm for the administrative benefits of surveillance and data-collection." (p 110) [66]

142. A number of witnesses told us about the approach taken in other European countries. Joerg Fedtke, Professor of Law, University College London, gave an account of the operation of the data protection legislation in Germany, pointing out that surveillance was ultimately regulated by reference to a strict constitutional commitment to the principle of proportionality. It is, he maintained, one of the key elements "which public authorities need to take into account in exercising their powers, whether surveillance, whether it is dealing with personal data, or whether it is any other function they might

---

[65] Lord Steyn, "Democracy, the Rule of Law and the Role of Judges", Attlee Foundation Lecture, 11 April 2006.

[66] See also Chapter 7.

perform." (Q 748) Dr Lee Bygrave, Associate Professor in the Faculty of Law, University of Oslo, told us that:

> "It is clear that if you look at, say, the Federal Republic of Germany, which arguably has the strongest protection for personal data in Europe, that constitutional platform has been very, very important for the case law of the Bundesverfassungsgericht [Constitutional Court] in curbing, particularly, the latest spate of surveillance measures being issued by the interior ministry in the Federal Republic, and, also, at Länder level." (Q 489)

143. The evidence we received suggests that, though there may be no consensus about whether there is a constitutional case for restricting the surveillance and data use activities of the state, consideration should be given to placing the rights contained in Article 8 of the Convention on a clear legal footing.

144. **We regard privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers as necessary conditions for the exercise of individual freedom and liberty. Privacy and executive and legislative restraint should be taken into account at all times by the executive, government agencies, and public bodies.**

The Data Protection Act 1998

145. The use of personal information is regulated by the Data Protection Act 1998 (DPA) which covers the circumstances under which personal information can be processed by public authorities and private organisations. Under the provisions of the DPA, any individual or organisation engaged in the handling of personal information is required to ensure that all information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with rights of data subjects under the Act;
- secure; and
- not transferred to other countries without adequate protection. (DPA 1998, Schedule 1)

146. So as to ensure that the processing of personal data is open and transparent, the Act establishes a system of notification (DPA 1998, Part III) whereby all organisations engaged in the handling of personal information are required to notify the Information Commissioner's Office (ICO) (unless they are exempt under the Act) and to provide details of the type of data processing being undertaken. This information is then published in the register of data controllers and is available for public inspection. Failure to notify is a criminal offence under the Act (DPA 1998, section 47). The objective of the system is that members of the public are able to find out who is processing personal information and for what purpose. The system is designed to ensure

that individuals are able to determine whether information relating to them is being held by another individual, government agency, or private organisation.

147. One of the key features of the regime established by the DPA is that it does not provide individuals with substantive rights that can be enforced by the courts. Instead, an individual who believes that his or her personal information is being improperly held or used must make a complaint to the ICO. According to the Act, the Information Commissioner has the power to:

- undertake assessments to check whether organisations are complying with the Act;
- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- serve enforcement notices and "stop now" orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- prosecute those who commit criminal offences under the Act;
- conduct audits to assess whether organisations' processing of personal data follows good practice; and
- report to Parliament on data protection issues of concern. (DPA 1998, Part V)

148. We took evidence on the operation and effectiveness of the DPA. In both his written and oral submissions, Richard Thomas, the Information Commissioner, gave an account of the work undertaken by his Office, and the challenges it currently faces as a consequence of advances in surveillance and data use technology. Although the Commissioner was keen to emphasise that he did not believe that "any sort of surveillance society is developing for malign reasons", he stressed that:

> "We think there is a need for much greater attention to be focused on the risks involved and the safeguards which are needed. We all now leave our electronic footprints in many places on a daily basis and as the pace accelerates our concern is to ensure that full consideration is given to the impact on individuals and society, that pre-emptive action is taken where necessary to minimise intrusion, and that measures are in place to safeguard against unacceptable consequences." (Q 2)

149. We discuss the role of the Information Commissioner in relation to the DPA in more detail in Chapter 5.

The Regulation of Investigatory Powers Act 2000

150. The third major piece of legislation we examined was the Regulation of Investigatory Powers Act 2000 (RIPA). Designed to replace the Interception of Communications Act 1985, RIPA established a framework for the use of surveillance and data collection techniques by the police, the security services, and other law enforcement agencies. In addition to criminalising the intercepting of a communication over a public network without consent or a warrant authorised by the Secretary of State,[67] the Act set out the

[67] According to section 5(3) of the Act, the Secretary of State can issue a warrant only if the surveillance proposed is necessary: (a) in the interests of national security; (b) for the purpose of preventing or detecting

circumstances under which public authorities—most notably the police—can engage in various types of surveillance activities. It provided a framework for the authorisation and review of those activities by the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner.

151. According to section 48(2) of the Act, surveillance is described as:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

152. Under RIPA, surveillance may be categorised as "directed" and/or "intrusive", with implications for whether a particular type of surveillance can be authorised. Although the definitions of directed and intrusive surveillance are complex it is possible to define them as follows.

Surveillance is directed if:

- it comprises covert observation or monitoring by whatever means;
- it is for the purpose of a specific investigation or specific operation (any crime or other offence); and
- it will or is likely to obtain private information about any person, not just the subject of the operation.

Surveillance is intrusive if:

- it is covert;
- it is carried out on any residential property or in any private vehicle; and
- it involves the presence of an individual on the premises or in the vehicle, or the use of a surveillance device.

Operation of the RIPA regime

153. There was disagreement between the Association of Chief Police Officers (ACPO) and the OSC as to the effectiveness of the current legal framework, and about the level of paperwork surrounding the system of authorisations. ACPO referred to a Review of RIPA commissioned in 2004:

> "The Review found the legislation had several ambiguities and deficiencies and had been implemented poorly. There was diverse interpretation and application of the law, and the training provided within the law enforcement community had been piecemeal … In particular, the Review identified a proliferation of unnecessary bureaucracy which was born of a generally 'risk-averse' approach. This risk-aversion meant, and continues to mean to this day, that there is little in the way of domestic case law to guide investigators and Senior Investigating Officers." (p 42)

---

serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom; or (d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement. http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

154. Although Assistant Chief Constable Nick Gargan, the former Chair of the Covert Investigation (Legislation and Guidance) Peer Review Group, stressed that ACPO regards RIPA as an effective piece of legislation, he also argued that:

> "The implementation of that piece of legislation has been difficult and it has created an excessive burden of unnecessary bureaucracy, which is the source of regular complaint from operational colleagues and commanders up and down the country ... We think that it is a fresh time to re-visit the legislation in its entirety." (Q 90)

155. Nick Gargan specified problems arising from legal ambiguity such as authorisations of surveillance in cases of joint activity between forces or where police were working with non-police staff, and the installation of intrusive surveillance cameras in private dwellings. In addition:

> "Unfortunately, one of the consequences of our own cultural risk aversion is that we tend to over-authorise. We have tried to look for sources of advice that would give colleagues the confidence not to over-authorise activity … Let us apply a little common sense, for example to the case where we send someone into an off-licence and ask him to try to buy four cans of lager so that we can prosecute the shop-keeper if he is selling inappropriately. Let us not dress that up as covert policing." (Q 128)

156. He went on to say that there was also a problem of contradictory advice being offered by the Information Commissioner and by the other Commissioners who have inspection powers under RIPA, and that "the fact of having separate bodies investigating largely the same field of activity creates a bureaucratic cost."(Q 132)

157. That the system of regulation established by RIPA was overly bureaucratic was rejected by the current Chief Surveillance Commissioner, Sir Christopher Rose. When asked whether the requirements set out in RIPA were overly onerous, Sir Christopher stated:

> "If you choose to class paperwork as bureaucracy, so be it, but one of the features of the paperwork connected with covert surveillance which is beneficial to everybody is if there is an impeccable paper trail showing what is sought, what is authorised, what renewals and cancellations there have been, that helps everybody." (Q 642)

158. Sir Christopher also suggested that the problems experienced by the police may be the result not of any deficiency in the legislation but its implementation:

> "So if ACPO or anybody else chooses to say there is far too much paperwork, one has to examine what that actually means. Sometimes, there is excessive paperwork because you will get an inexperienced police officer, for example, who is unduly repetitive either in what he is seeking to have authorised or in what is authorised. That is to be remedied, as it seems to me, by training the relevant officer to do his job better." (Q 642)

159. **We recommend that the Government undertake a review of the administrative procedures set out in the Regulation of Investigatory Powers Act 2000 so as to resolve the contrasting views expressed by the Association of Chief Police Officers (ACPO) and the Office of**

Surveillance Commissioners about the effectiveness of the current legal framework and the system of authorisations.

160. Concerns were expressed by Liberty that the system for approving both directed and intrusive surveillance operations is insufficiently robust and independent, with operations capable of being approved internally by the police and the security services:

> "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." (p 106)

161. Professor Feldman questioned the wisdom of allowing the intelligence services to be able to authorise their own surveillance activities in the absence of checks and balances. Although he acknowledged that the Investigatory Powers Tribunal (IPT) had the power to review the legality of such authorisations, he doubted its effectiveness:

> "I think the Investigatory Powers Tribunal has yet to prove itself—it has not had enough to do yet perhaps to be clear just how effective it is going to be—but I am a little bit worried about the extent to which these intrusive or relatively extensive activities can be authorised by a senior official of the agency that is going to carry out the activity without the need for external independent scrutiny in all cases." (Q 560)

162. We are concerned about the level of independent and effective oversight of surveillance activities under RIPA. Although we accept that the OSC provides oversight, and the assurances of Sir Christopher Rose that the inspection system has helped to improve police practices, we consider that more should be done to protect the privacy of individuals from over-zealous state surveillance. We were concerned to hear from Hugh Tomlinson that the law provides little in the way of redress where surveillance powers have been exceeded. (p 442)

163. **We recommend that the Government consider introducing a system of judicial oversight for surveillance carried out by public authorities, and that individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result. We recommend that compensation should be available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers conferred by the Regulation of Investigatory Powers Act 2000.**

Local authority powers under RIPA

164. During the course of the inquiry there were well-publicised examples of local authorities using the surveillance powers under RIPA to stop fly tipping, reduce dog fouling, and investigate fraudulent school place applications. David Holland, holder of the consumer protection brief for Cardiff Council, denied that local government had systematically abused its power:

> "The Council can undertake what we call directed surveillance, but our powers are quite limited in what we can do … Most of a local authority's

duties are placed upon it by regulation and most of what we do in administering that legislation is done overtly" (QQ 789, 793).

165. He also told us:

> "I think we have said that our role as a council is to protect and serve the local community. I will be frank with you; I will use every power I have available to do that because there are some real rogues out there that prey on the vulnerable and elderly … I will use whatever powers I have available to bring those people to book, but … I will work within RIPA and I will make sure that if my officers choose to undertake or apply for directed surveillance that that application is an absolutely necessary use of that power and that it is a proportionate response." (Q 789)

166. These points were echoed by Donna Sidwell of the Local Authority Coordinators of Regulatory Services (LACORS):

> "There are certainly different degrees of seriousness … We would argue that the checks and balances already in place are fairly good at enabling a local authority to assess on necessity and proportionality grounds. There are some occasions when you may challenge the decisions that have been taken and you might say that if you were looking at it from the judicial perspective a different decision might have been taken. I think there are areas where additional guidance can assist and working with the Home Office, the Office of Surveillance [Commissioners] and the Office of the Interception Commissioner can help us in that … We want the local authority communities and residents to be confident and to believe that they are not being snooped on. We strongly do not believe that is the case." (Q 794)

167. She also told us that:

> "There will be those occasions where it is more appropriate for covert surveillance to be used, for a covert human intelligence source to be authorised or for subscriber or billing information to be obtained. (Q 794)

168. Professor Janice Morphet, a former local authority officer and Chief Executive, observed that covert surveillance was, for example, a traditional Trading Standards practice with regard to market stalls, dumping, and off-licence sales to minors:

> "The ones you have described in terms of schools and refuse are much more difficult to deal with. I do not think it needs covert surveillance … I would send an inspector along with the refuse collection team. I do not think I would make that person covert … Thinking about schools … I do not think I myself would go down that line … but what we have to recognise is that at local level this is the kind of issue that will absolutely fill the chief executive's postbag and that of the local members. I am not defending [covert surveillance] because I think I would try other things." (Q 918)

169. Councillor Hazel Harding, Leader of Lancashire County Council and Chair of the Local Government Association Safer Communities Board, said:

> "From an elected member's point of view, I am appalled when I see some of those examples in the press as well … It is a case, in some instances, of using a sledgehammer to crack a nut." (Q 807)

170. The Minister of State at the Home Office for Crime, Policing, Counter-terrorism and Security, Vernon Coaker MP, said that some such uses of RIPA powers were "inappropriate", and that he was working with the Department of Communities and Local Government (CLG) to look "at what we need to do to ensure that the powers are used appropriately and in a way which commands the respect of the public", in order to "stop some of these other things happening which undermine that support." (Q 1019) He added that "we need to look at the codes of conduct and see how we take them forward." (Q 1029) He also told us that Sir Simon Milton, the then Chairman of the Local Government Association (LGA), had written to local authorities to tell them "that when they used these powers they had to make sure they were used in a necessary and proportionate way and reminded them that that is in the guidance and that is what they should be doing." (Q 1022) The Minister referred to the use of RIPA powers "to tackle serious criminals":

> "North Yorkshire County Council used directed surveillance and communications data authorised by RIPA to prosecute three roofers who had persuaded 11 elderly victims to pay for unnecessary work on their roofs. These victims lost in excess of £150,000, two of the 11 victims lost their entire life savings, and the three criminals responsible were sentenced to between three, five and six years." (Q 1019)

171. Such controversy led us to re-examine how local authorities came to possess such powers in the first place. Vernon Coaker explained that in the Act as passed in 2000, local authorities were not included in the list of public authorities that could have access to communications data. (p 360) During the passage of the Act, Bill Cash MP wrote to the then Home Secretary in relation to concerns raised with him that the Bill as drafted would extend the power to "a range of officials in several public-sector bodies including local authorities and … government departments."[68] The then Minister of State, Charles Clarke MP, wrote back to Mr Cash, explaining that such concerns "may be referring to the provision in the Bill allowing for the Secretary of State to make further additions to" the list of relevant public authorities with power to obtain data "at some future stage if it is deemed necessary … by means of the affirmative resolution procedure. I can, however, confirm even at this stage that such powers will not be made available to local authorities."[69]

172. However, in the new Parliament in 2003 two Orders were passed by affirmative resolution in both Houses that gave a number of additional public authorities, including local authorities, access to communications data and the power to use directed surveillance and covert human intelligence sources within the RIPA regime.[70] The Orders were passed after a period of public consultation.[71]

---

68 See http://cryptome.org/clarke-rip-lie.pdf

69 ibid.

70 Statutory Instrument 2003 No. 3172 The Regulation of Investigatory Powers (Communications Data) Order 2003; and Statutory Instrument 2003 No. 3171 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.

71 Home Office, Access to Communications Data—Respecting Privacy and Protecting the Public from Crime, March 2003.

173. Vernon Coaker agreed that Charles Clarke had "confirmed that there was no intention to extend the provisions in RIPA to enable local authorities access to communications data." The Minister argued that "this was because a number of public authorities, including local authorities, already had access to communications data either by arguing individual exemptions under the Data Protection Act 1998 or by other statutory powers". He added that the decision to introduce the 2003 Order was made when "it became clear that a more systematic approach was required that ensured public authorities were subjected to the same regime and to ensure a more consistent and accountable approach to all aspects including authorisations, consideration of necessity and proportionality, independent oversight and appeals mechanisms." (p 361)

174. Vernon Coaker subsequently elaborated on this, telling us that "the change of heart came because of a recognition of the problem that arose about the inconsistency of approach that was taking place. Some people were approaching internet service providers through RIPA legislation; others, like local authorities, were approaching them to get exactly the same information that they get under RIPA through other legislation, through the Data Protection Act, some of the exceptions that exist there, or through production orders under PACE [Police and Criminal Evidence Act 1984] … that is why we then went out to public consultation to say, 'Look: this is the situation. Would it not be better to include local authorities therefore within that?'" (Q 1012) He also attempted to reconcile Charles Clarke's categorical assurance with the Government's later desire for consistency: "Clearly, if an assurance has been given you like to try and ensure that that assurance is maintained, but … sometimes there are things that happen two, three, four, five, six years later … despite the assurance that was made there is a need to change". (QQ 1017, 1018)

175. We are concerned lest this reversal set a precedent for future unforeseen policy changes in the field of surveillance.

176. The situation regarding directed surveillance and covert human intelligence sources is also complicated. Local Authorities exercise their powers in this area under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003. The debates in both Houses of Parliament when the Order was approved in 2003 seemed to indicate that these were not new powers.[72] We wrote to Vernon Coaker on 18 December to seek clarification of this point. His response of 12 January confirmed that these were not new powers: prior to RIPA, the use of directed surveillance or covert human intelligence sources by any public authority, including local authorities, was unregulated. The Minister explained that RIPA addressed the situation and was designed to ensure that public authorities complied with the ECHR. (p 337)

177. We are concerned at the use by some local authorities of their surveillance and communication data collection powers under RIPA. We were pleased to note that the Home Secretary had announced a Government consultation on proposed changes to RIPA including revisions to the Codes of Practice that come under the Act, a consideration of which public authorities should exercise powers under RIPA and the possibility of the method by which

---

72 HL Deb 13 Nov 2003 cols 1521–62 and 1573–1604, and House of Commons Third Standing Committee on Delegated Legislation on 4 Nov 2003 (cols 3–38).

RIPA powers are authorised being changed.[73] **We recommend that the Government consultation on proposed changes to the Regulation of Investigatory Powers Act 2000 should consider whether local authorities, rather than the police, are the appropriate bodies to exercise such powers. If it is concluded that they are the appropriate bodies, we believe that such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years. We recommend that the Government take steps to ensure that these powers are only exercised where strictly necessary, and in an appropriate and proportionate manner.**

178. We examine in more detail the question of the training of local authority personnel in Chapter 6.

The National DNA Database

179. The National DNA Database (NDNAD) was established in 1995 in England and Wales (Scotland and Northern Ireland have their own databases), and contains profiles derived from DNA samples taken from anybody over ten years old arrested for a recordable offence (whether or not they are subsequently charged or convicted),[74] from volunteers and from crime scenes. It is not governed by one particular piece of legislation, although various acts have supported its establishment and development over the years. We consider the consequences of this fragmented system of regulation later in the report. [75]

180. The NDNAD, in proportionate terms, is the largest of its kind in the world. It contains DNA profiles of 7.39 per cent of the UK population, according to Vernon Coaker. (Q 1049) Austria's forensic DNA database is the next largest in proportionate terms, and contains about one per cent of the population, while the USA's FBI "CODIS" database contains about 0.5 per cent.[76] The Nuffield Council on Bioethics states that "the threshold for holding DNA profiles on a forensic database is far lower in the United Kingdom than in any other Member State of the EU, and the proportion of the population included on the UK DNA Database is correspondingly far higher than in other EU countries."[77] England and Wales are alone in the EU in systematically retaining the profiles or samples of individuals who have not been convicted of a crime.[78] However the recent judgment in the case of *S. and Marper v. the United Kingdom* ruled that this practice was not compatible with the ECHR. We discuss this in more detail at paragraph 194.

181. Since the establishment of the NDNAD, the use of bioinformation—especially DNA profiling—has increased substantially, for instance in crime detection, the investigation of offences and the conduct of prosecutions, and

---

73 Jacqui Smith MP, Speech to the Intellect Trade Association, 16 December 2008.

74 A recordable offence is any offence for which the police are able to keep records of convictions and offenders on the Police National Computer.

75 Police and Criminal Evidence Act 1984; Criminal Justice and Public Order Act 1994; Criminal Evidence (Amendment) Act 1997; Criminal Justice and Police Act 2001; Criminal Justice Act 2003; and Serious Organised Crime and Police Act 2005.

76 The Forensic Use of Bioinformation: Ethical Issues, op. cit., para 1.22.

77 ibid., Executive Summary, p xxiv, para 47. See p 52, Box 4.3 for comparisons of Member States' practices.

78 ibid., p 52, Box 4.3.

the identification of deceased persons and body parts. The Prime Minister has praised DNA as "one of the most effective tools in fighting crime."[79] Other witnesses agreed that the NDNAD could be a useful tool. The Nuffield Council on Bioethics argued that "well-functioning forensic databases have the potential to promote the public interest to a significant degree" and that "the science and technology of DNA profiling is increasingly robust and reliable".[80] GeneWatch UK told us that the NDNAD is "an important tool in criminal investigations" (p 72), whilst Liberty also affirmed the NDNAD's utility, given proper justification and proportionality.[81]

182. Chief Constable Peter Neyroud, Chief Executive of the National Policing Improvement Agency (NPIA), the custodian body for the NDNAD, has stated that "the Database continues to grow in significance as a national intelligence resource in support of policing."[82] He told us that in cases of "serious offences and particularly serious violent offences … these databases are incredibly important in the investigation." (Q 108) He added that Ian Huntley, found guilty of the 2002 murder of two girls in Soham, "was arrested a considerable number of times before the events of Soham for offences that ranged between relatively minor potential sexual transgressions to quite significant ones. Mr Huntley would have, under the Criminal Justice Act 2003, appeared on the database. Prior to that he did not. That would have been a significant benefit to the investigation". (Q 113) He also told us that "the Police Service's case to Government when the last changes to the database were made was about the strong likelihood of serious crime detections that were there as a result of expanding the envelope beyond those who were convicted of a recordable offence or cautioned. That has indeed proved to be the case." (Q 120)

183. Tony McNulty told us that the NDNAD enables perpetrators of a crime to be brought to justice—sometimes decades after the crime has taken place. (Q 960) His successor, Vernon Coaker, justified the NDNAD's size on the basis that "it has enabled us to solve a significant number of serious crimes. If you look at the numbers of murders, rapes, serious robberies and other violent crimes that have been solved as a result of having that database, we think that in the end is a proportionate response to tackling crime and it is a justification for it." (Q 1052) He further told us that, between May 2001 (when the provisions of the Criminal Justice and Police Act 2001 came into effect) and December 2005, approximately 200,000 profiles were retained that would have to have been removed prior to the passing of the Act. Of these, "approximately 8,500 profiles from some 6,290 individuals have been linked with crime scene profiles involving nearly 14,000 offences." (Q 1056) The Minister was unable to clarify, however, how many of these profiles had directly led to a conviction. (QQ 1057–60)

184. On the other hand, Dr Helen Wallace, Director of GeneWatch UK, took issue with some of the claims made. She disputed Tony McNulty's emphasis on the value of the retention of individual DNA samples as opposed to the re-analysis of crime scene evidence, and also asserted that there have been

---

79 Gordon Brown MP, Speech on Security and Liberty, 17 June 2008.

80 The Forensic Use of Bioinformation: Ethical Issues, op. cit., Executive Summary, p iii, paras 3, 5.

81 Overlooked, op. cit., p 67.

82 National Policing Improvement Agency, *Annual Report 2006–07*, p 6.

occasions when "DNA matches have been confused with successful prosecutions, or that irrelevant cases have been cited in support of retaining innocent people's DNA." (pp 94–102)

185. The Nuffield Council on Bioethics identified some of the possible dangers of relying on the NDNAD: "Deliberate or accidental contamination, misinterpretation of mixed samples (those originating from more than one person), mistaken interpretation of partial profiles and the misuse of statistics to establish the probability of a match."[83] Professor Peter Hutton, Chairman of the National DNA Database Ethics Group, further mentioned incomplete crime scene samples, the physical degradation of DNA, and the important element of laboratory technicians' judgment in comparing samples as factors that detracted from the forensic utility of DNA. (QQ 162–63)

186. The effectiveness or otherwise of the NDNAD in solving crimes should not be the only consideration when considering the appropriateness of the current arrangements; also relevant is whether law-abiding citizens who have never been convicted of a crime are unfairly disadvantaged by being included on the Database. Dr Wallace believed that there were disadvantages because the purpose of retention is "to look for matches with any potential future crime scene profile" so that it is "a kind of biological tagging" which resulted in people being treated as "suspect[s] for any **future** crime." There was also a "potential threat to 'genetic privacy' if information is revealed about health or family relationships" and "potential for unauthorised access, abuses and/or misuses and mistakes: including the tracking of individuals and their relatives". (Q 168 and pp 97, 99) DNA profiles could potentially be used "to try to identify whether [somebody] has been present at scenes other than crime scenes (for example, a political or religious meeting)." (p 74)

187. The Royal Academy of Engineering (RAE) suggested that the retention of DNA profiles for use in future investigations could be contrary to the DPA and that such profiles constituted "sensitive personal information that an individual should have the right to withhold if there is no specific need for it in the investigation or prevention of crime." (p 436)

188. Some witnesses had concerns about possible discrimination. As Professor Hutton told us, "at the moment there are some groups who are hugely over represented on the database in relation to their population incidence in society in general", particularly black youths. (Q 189) Both Professor Graeme Laurie of the University of Edinburgh Law School (who contributed to the Nuffield Council on Bioethics' report on *The forensic use of bioinformation: ethical issues*) and Dr Wallace agreed that the number of ethnic minority people on the database did not reflect the number that had actually committed crimes. (QQ 192, 193) Professor Hutton suggested that this over-representation was "related to the stop and search policy which is occurring in community policing". (Q 189)

189. By contrast, the NPIA argued that "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." (p 46) Tony McNulty insisted that "there are no guilty people on [the NDNAD] in the sense of guilty of future charges" and that "it is not an information source for all the naughty and potentially nasty people in the country … It is purely an

---

[83] The Forensic Use of Bioinformation: Ethical Issues, op. cit., Executive Summary, p. xiii, para 3.

informational and investigatory device for the police." (Q 960) He dismissed the suggestion that the Government was saying that "we have all these people on the database, they all must be guilty, now let us find a crime to attach to them" and told us that "I do not think there is a matter of principle here; I do not think there is any stigma attached at all with being on the database." (QQ 964–65) We were therefore puzzled by his declared opposition to a universal database on the grounds of "practical civil liberties" as well as "potentially legal concerns". (Q 966)

190. We believe that the retention of the DNA profiles of people convicted of a recordable offence can be justified, although GeneWatch UK called for the reintroduction of "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". (p 76) In her speech of 16 December 2008 the Home Secretary said:

> "We will consult on bringing greater flexibility and fairness into the system by stepping down some individuals over time—a differentiated approach, possibly based on age, or on risk, or on the nature of the offences involved … The DNA of children under 10—the age of criminal responsibility—should no longer be held on the database … and we will take immediate steps to take them off."[84]

We welcome this commitment by the Government.

191. Another pressing issue is the retention of the DNA profiles of people arrested for or charged with a recordable offence but not subsequently convicted—in other words people who are, in the eyes of the law, innocent of any crime and who should arguably be treated the same as people who have never been arrested.

192. During the course of the inquiry we learned that in other jurisdictions the profiles of innocent people are generally not retained. For example, the American Civil Liberties Union (ACLU) told us that an argument is now being conducted in some US states over whether individuals who are arrested should have their profiles added to the database—but, unlike in the UK, most states pursuing this path were also specifying that an arrestee's profile should be removed if he or she is not charged or convicted of an offence.[85]

193. We heard evidence on this point from several witnesses. Most recently, Vernon Coaker told us that the retention of such profiles was "appropriate", "proportionate", and "a response that commands the support of the population." (Q 1055) He added that, where such profiles are retained, there was "an appropriate threshold" because "police officers can only arrest somebody if they act in accordance with the PACE code, and the PACE code requires a police officer to have at least a reasonable suspicion that the person they have arrested has committed an offence. That offence has to be of the standard of a recordable offence … It is a proportionate response to the question, is it possible that some of the people who come into contact with the police in the way that I have said may be people who it would be beneficial in terms of the public good for their DNA to be retained." (QQ 1055, 1064–65)

---

84 Jacqui Smith MP, Speech to the Intellect Trade Association, *op. cit.*

85 Appendix 4, para 60.

194. Shortly after Vernon Coaker's statement, the judgment of the European Court of Human Rights on 4 December 2008 in the case of *S. and Marper v. the United Kingdom*, was delivered. The case was brought by two individuals: one was arrested for and charged with, but acquitted of a recordable offence; the other was arrested for and charged with a recordable offence, but the case was formally discontinued. Both wanted their DNA to be taken off the NDNAD. The Court ruled that the Government's current policy breached Article 8 of the European Convention on Human Rights.[86] On 16 December 2008 the Home Secretary announced that the Government would produce a White Paper on forensics which would deal with the arrangements for DNA retention. She asserted that "we've seen convictions for serious crimes of culprits who had had their DNA taken and retained for a previous crime where they were arrested, but not convicted."[87]

195. GeneWatch UK drew our attention to the regime in Scotland:

> "The Scottish Parliament voted against indefinite retention of DNA profiles and samples from persons acquitted or not proceeded against, in May 2006. Instead, police powers were expanded to allow temporary retention (for up to 5 years, with judicial oversight) from a much smaller number of people who had been charged but acquitted of a serious violent or sexual offence. The Scottish Government is currently conducting a review of this decision in order to assess whether the temporary retention of data from this more limited category of unconvicted persons is appropriate. In conducting its review, the Scottish Government has expressly ruled out the indefinite retention of fingerprint and DNA data acquired from individuals who are not convicted of any crime." (p 98)

196. We believe that the retention of DNA profiles on the NDNAD potentially impinges on civil liberties. DNA profiles provide the state with large amounts of personal information about its citizens that could, in the future, be used for malign purposes.

197. **We believe that DNA profiles should only be retained on the National DNA Database (NDNAD) where it can be shown that such retention is justified or deserved. We expect the Government to comply fully, and as soon as possible, with the judgment of the European Court of Human Rights in the case of *S. and Marper v. the United Kingdom*, and to ensure that the DNA profiles of people arrested for, or charged with, a recordable offence but not subsequently convicted are not retained on the NDNAD for an unlimited period of time.**

198. In our view, it would only be acceptable to retain the DNA profiles of innocent people indefinitely if there were a universal DNA database containing the profiles of everybody in the country. However, this potential solution to the anomalous system which currently prevails was criticised by the Information Commissioner:

> "I think both for practical and civil liberties reasons I am really quite sceptical about the logic of saying that there are some unfair discriminations there at the moment and therefore we resolve that by having everyone's data on a mandatory basis." (Q 11)

---

86 For the text of the judgment see http://www.bailii.org/eu/cases/ECHR/2008/1581.html

87 Jacqui Smith MP, Speech to the Intellect Trade Association, op. cit.

199. Tony McNulty, who agreed with the "logic" of a universal database, nonetheless thought that it would be "intrusive and unnecessary and cause all sorts of difficulties" and would carry implications in terms of costs and practicalities. (QQ 960, 962, 967) His successor, Vernon Coaker, told us that he would not find a universal database acceptable:

> "The Government's view at the present time is that a [universal] national DNA database, notwithstanding some of the benefits that might accrue, is not a proportionate response and is not something that would necessarily command the support of the population." (Q 1061. See also QQ 1054–55)

200. **Whilst a universal National DNA Database would be more logical than the current arrangements, we think that it would be undesirable both in principle on the grounds of civil liberties, and in practice on the grounds of cost.**

201. Finally we consider the retention of DNA profiles of witnesses or victims of crime who volunteer to give a DNA sample to help in a police investigation and then find that their DNA becomes part of a permanent record because of the choice they have made when giving the sample. Professor Hutton told us that there were some 16,000 such samples at the end of 2006 (Q 179), whereas Vernon Coaker gave a figure of 32,000 volunteers. (p 375) Peter Neyroud conceded that "there are some issues there around making sure people are properly informed at the time the sample is taken." (Q 113) He explained that:

> "In respect of volunteers, the process is that they can choose to have their DNA sample destroyed or consent to the profile being loaded on to the DNA database." (Q 115)

202. However, Professor Hutton explained:

> "The method of taking consent is probably on occasions flawed in that the person taking consent from an individual may not meet the basic criteria in common law to be able to answer specific questions about what is going to happen to the sample and the processes it will go through." (Q 172)

203. Professor Hutton went on to describe the procedures for gaining the consent of volunteers:

> "The current consent form in fact has on it two options. One is to sign so that the DNA and its derived data will only be used for that case; the second is to sign to say that it can be used for that case and the second sample retained and the DNA profile loaded on to the National Database". (Q 172)

204. Professor Laurie addressed the question of whether volunteers should be asked if they are willing for their samples to be retained once an investigation is completed:

> "I think that may be a possible approach on certain conditions: first of all that it is demonstrated that that would actually further the ends of prosecution services to have volunteers who are effectively innocent persons by retaining that information. Secondly, that it would respect the fundamental tenets of the law of consent, being informed consent, that you were fully informed … of what were the consequences of you being kept on this if it is indefinitely. Thirdly, hopefully it is not

> 'indefinitely' because your right to refuse, again a fundamental tenet of the law of consent, should be respected, whereas at the moment it is not." (Q 178)

205. The NDNAD Ethics Group has recognised the seriousness of this matter and has given it a prominent place in its work programme, where it has generated important recommendations.[88] Professor Hutton said that the Ethics Group prefers that volunteer samples should only be used for the case in hand, especially as research evidence suggests that, in most cases, there would be no loss to operational policing if the samples were not placed on the NDNAD. He added that "our work on this has been completely supported by ACPO". (Q 172)

206. A further issue relating to DNA profiles of volunteers is when and whether such profiles should be deleted from the NDNAD. Such profiles are only loaded on to the NDNAD if the volunteer gives his or her consent. But, as Professor Hutton told us, once the profile is loaded onto the NDNAD, "it is there for 100 years and it is very difficult to get off; and removal is subject to the individual decisions of local Chief Constables." (Q 172) Similarly, Gareth Crossman warned us that profiles "only tend to be deleted when an individual is so bloody-minded about it that they continue to push and push until in the end the individual police force gets rid of it." (Q 264)

207. Professor Hutton suggested that there would be few drawbacks to making it easier to have volunteer profiles deleted because, as a recent piece of work undertaken by the Ethics Group and ACPO had shown, "if, in the main, for the majority of cases volunteer samples were not loaded on to the National Database and were used only for the case in hand there would be no loss to operational policing." (Q 172) Tony McNulty suggested that he was open to this idea, telling us that "the notion that volunteers should have at least the option for retention being for a shorter period than forever is a fair one that we are exploring." (Q 970)

208. **We recommend that the law enforcement authorities should improve the transparency of consent procedures and forms in respect of the National DNA Database (NDNAD). We believe that the DNA profiles of volunteers should as a matter of law be removed from the NDNAD at the close of an inquiry unless the volunteer consents to its retention.**

Regulation of the National DNA Database

209. The lack of a single legislative framework for the NDNAD worried a number of witnesses. Professor Laurie told us:

> "We now have multiple pieces of legislation which need to be fitted together in order to understand exactly what is going on … what is missing is independent, accountable and powerful oversight; a fundamental reappraisal of the basis of the National DNA Database; a suitable framework for its development, its management and governance—which is not actually in law at the moment—clarity of purpose and also articulation of the values that actually underpin this, which are lost in this morass of laws … consolidation of this entire field of law would seem most appropriate." (Q 198)

---

88 1st Annual Report of the Ethics Group: National DNA Database, op. cit., paras 5.2–5.20.

210. Professor Hutton agreed with Professor Laurie that "there should be a better statutory basis" and noted that this argument had been made by the Ethics Group. (Q 208) He thought it was unsatisfactory that "the situation that exists is outside any national regulatory framework and has many elements of judgment in it." This means, for example, that "although the police can take samples and load them on to the database there is actually no compulsion on the police to take a sample when somebody is arrested, and once arrested and the sample has been taken there is no compulsion for it to be loaded [onto the NDNAD]—it is entirely at the discretion of the police." (Q 180) Dr Wallace also agreed that the NDNAD should be put on a specific statutory basis. (Q 204) The House of Commons Home Affairs Committee has backed this view, recommending that "alongside any conclusions of the PACE review the Government introduce primary legislation to replace the current regulatory framework for the National DNA Database".[89]

211. The RAE thought that, in formulating new legislation, consideration should be given to establishing "a new body to oversee the collection, retention and use of bioinformation … [and] to check that records are not kept for excessive periods or without clear justification. Alternatively, the role of the Surveillance Commissioner could be extended to cover the collection, retention and use of bioinformation by the police service." (p 436)

212. **We are concerned that the National DNA Database (NDNAD) is not governed by a single statute. We recommend that the Government introduce a bill to replace the existing regulatory framework, providing an opportunity to reassess the rules on the length of time for which DNA profiles are retained, and to provide regulatory oversight of the NDNAD.**

Regulation of CCTV

213. At present, there are few restrictions on the use of public area CCTV cameras in the UK. According to paragraph 1.4 of the Covert Surveillance Code of Practice, the provisions of RIPA do not apply to CCTV systems unless they are being used for a pre-planned surveillance operation.[90] While the DPA regulates the handling, storage and processing of information obtained via CCTV, it does not place any restrictions on where such cameras can be installed in public or under what circumstances. Provided that they comply with the relevant planning restrictions, public authorities such as local councils are free to install CCTV systems in town centres and other public places (such as residential estates) without prior approval from central government or the permission of residents. Furthermore, as the DPA only governs how information that has been recorded and stored is dealt with, in principle it does not apply to situations where cameras are used for observation only and where no recording is made. As a consequence, local authorities and the police are in principle free to use CCTV cameras for general, unrecorded surveillance.[91]

---

89 A Surveillance Society?, op. cit., para 285.

90 Home Office, Covert Surveillance—Code of Practice, 2002.

91 The use of CCTV cameras by private organisations—such as banks and retailers—is typically assumed to be authorised under section 3 of the Criminal Law Act 1967 on the grounds that it constitutes a reasonable means to prevent crime.

214. Both Liberty and JUSTICE expressed serious concerns about the fact that CCTV remains largely unregulated. Noting that the DPA was not intended to provide a comprehensive framework for CCTV regulation, Liberty argued that new data protection legislation was needed to reflect changes in the technology of visual surveillance and to regulate better the use of cameras. (pp 105–08) Liberty also drew attention to a statement released by the Council of Europe in March 2007, which suggested that strong regulation was necessary if human rights were to be protected from overly intrusive CCTV surveillance:

> "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 [to the individual's] 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." (p 106) [92]

215. JUSTICE also pointed to the inadequacy of the existing legislative regime, and suggested that it is a mistake to suppose that existing privacy safeguards—such as the DPA or RIPA—are capable of providing effective protection. (pp 111–12)

216. We received a number of suggestions as to how the existing regulatory structure could be reformed and CCTV better controlled. According to Dr Andrew Adams of the School of Systems Engineering, University of Reading, the principal regulator for CCTV should be the OSC, whose "role and resources should be expanded to provide licensing for public space CCTV schemes, guidelines on their deployment and operation and audit of the adherence to these guidelines." If video footage were processed in such a way as to transform it into personal data, the OSC should work closely with the ICO to ensure adherence to the data protection principles laid down in the DPA. (p 382)

217. The RAE suggested that in order to address an imbalance of power between the citizen and the state as regards the use of CCTV, an element of "reciprocity" should be introduced. This, they argued, could be achieved by allowing the public access to detailed information about the positioning of cameras, and the launch of a website "containing maps which indicate the locations of cameras, and sample images from cameras demonstrating their range. This would allow individuals and communities to raise complaints should they feel that particular cameras are unnecessary or excessively intrusive." (p 434)

218. Vernon Coaker told us that "the Government agrees with the recommendation in the National CCTV Strategy, that there should be a national body for the governance and use of CCTV in this country, and we will be looking to establish one. I cannot give a timeframe for that". (Q 1069) On the question of statutory regulation, he added that "it is not something that we would necessarily dismiss but in the first instance we want to establish the national body and see how that works with respect to voluntary

---

[92] European Commission for Democracy Through Law (Venice Commission), Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights, March 2007, paras 79, 81, http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

regulation, keeping in our back pocket the need, if necessary, to do more." (Q 1069)

219. **We recommend that the Government should propose a statutory regime for the use of CCTV by both the public and private sectors, introduce codes of practice that are legally binding on all CCTV schemes and establish a system of complaints and remedies. This system should be overseen by the Office of Surveillance Commissioners in conjunction with the Information Commissioner's Office.**

CHAPTER 5: REGULATORS

Introduction

220. In this chapter we consider the roles played by the various commissioners who oversee surveillance and data use, and suggest how their oversight functions might be enhanced. Our focus is primarily on the Information Commissioner, who has by far the broadest remit, but we also look at the other commissioners who oversee the use of powers under the Regulation of Investigatory Powers Act 2000 (RIPA). The remit of the commissioners is set out in Box Two.

BOX 2

The Commissioners

The Information Commissioner: oversees and enforces the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations, as well as the Freedom of Information Act 2000 (FOIA).

The Chief Surveillance Commissioner: leads the Office of Surveillance Commissioners (OSC), which provides oversight of the conduct of covert surveillance and the use of covert human intelligence sources (CHIS) under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Police Act 1997.

The Interception of Communications Commissioner: keeps under review the issue and operation of warrants permitting interceptions and the acquisition of communications data under RIPA.

The Intelligence Services Commissioner: reviews the issue by the relevant Secretary of State of warrants and authorisations for operations by the Security Agencies and Ministry of Defence (MOD) which fall under his oversight, namely warrants issued under the Intelligence Services Act 1994 and warrants and authorisations for surveillance and agents under RIPA.

The National Identity Scheme Commissioner: to be appointed in 2009. Will review the arrangements made by the Secretary of State and by designated authorities for the purposes of their functions under the Identity Card Act 2006 or its subordinate legislation; the arrangements made, by persons to whom information may be provided, for obtaining the information available to them and for recording and using it; and the uses to which ID cards are being put.

The Information Commissioner

221. The Information Commissioner is responsible for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He promotes the protection of personal information by increasing public awareness and by providing guidance to individuals and organisations, and he takes remedial action when the DPA is breached.

222. The responsibilities of the Information Commissioner's Office (ICO) have been especially onerous since the advent of FOIA. In many other countries and jurisdictions where there is a statutory basis for data protection and freedom of information, these roles are divided between separate Commissioners, although views differ on whether or not they are best

combined. This issue had been debated recently in Canada, where there are separate Commissioners at the federal level, but we learned that a merger had been rejected largely owing to the strong interest in privacy (especially in the light of 9/11), and also because the tension between the principles of privacy and access to information made it preferable to represent people's rights separately in each of these fields. Both Commissioners, it was said, should share a mandate to educate the public.[93]

223. We were struck by the number of witnesses who called for an expansion in the role of the Commissioner and for his powers and resources to be increased. The Foundation for Information Policy Research (FIPR) suggested that "the Information Commissioner's Office was designed to be weak". (p 404) Yet the overwhelming impression we received was that, given the impressive work that is currently being done by the Commissioner's Office, there is a pressing need to strengthen his regulatory hand. Dr David Murakami Wood, Lecturer at the School of Architecture, Planning and Landscape, University of Newcastle upon Tyne, and representative of the Surveillance Studies Network, told us that:

> "We regard the current Information Commissioner as being an extremely active and effective regulator who has gone in some ways way beyond what he needed to do and has indeed sparked this whole debate in the first place. He is shackled in the sense that his powers are limited and indeed the powers of his office are limited." (Q 68)

224. We also heard from a number of witnesses about the powers made available to other Commissioners in comparable European jurisdictions. While the Information Commissioner is by no means an especially weak regulator and has been provided with an array of powers, it was also apparent that other countries such as Germany have provided his counterpart with considerably more authority. (Professor Fedtke, Q 739)

225. The Information Commissioner, Richard Thomas, made a strong case for a number of changes to the current regulatory regime, both in terms of the requirements that should be placed on organisations responsible for handling personal data, and the powers available to the Commissioner's Office to enforce the provisions of the DPA. Specifically, he suggested five key ways in which the current legal regime could be substantially strengthened and improved:

(1) mandatory Privacy Impact Assessments (PIAs) by government departments;

(2) requirements to have codes of practice in place for proactive information sharing in the public sector;

(3) proper consultation with the Commissioner before significant new developments;

(4) increased audit and inspection powers for the Commissioner; and

(5) effective penalties for serious disregard for the requirements of the data protection principles. (p 6)

---

[93] Appendix 4, para 28.

Codes of practice

226. The 2008 *Data Sharing Review Report*, by Richard Thomas, the Information Commissioner, and Mark Walport, Director of the Wellcome Trust (the Thomas-Walport Review), proposed that the Information Commissioner should have a statutory duty to produce and periodically update a data-sharing code of practice—to be laid before and approved by Parliament—and "to endorse context-specific guidance that elaborates the general code in a consistent way."[94] Although the Commissioner has already published a *Framework Code of Practice for Sharing Personal Information*, in October 2007, it has no statutory basis and is not subject to any parliamentary oversight. The proposed system, by contrast, "would provide greater clarity and introduce greater scrutiny."[95]

227. The Code, as envisaged, would "establish standards setting out how organisations involved in sharing personal information should handle and protect the data under their control" and "apply to all those involved in data sharing, who should adhere to it as a matter of good practice and consider it as an authoritative interpretation of the relevant data protection principles." While breaches of the Code would not be against the law, it "should have suitable authority and be sanctionable in the sense that the Commissioner and the courts should be expressly entitled to take non-compliance with its provisions into account when deciding whether data controllers have complied with the data protection principles."[96]

228. We are pleased that the Government have agreed that the Information Commissioner should be placed under a statutory duty to produce a data-sharing code of practice which would be approved by Parliament.[97] In our view, this should result in a Code that would be an authoritative guide to those involved in data sharing. The role of Parliament in approving this Code would bring greater transparency to the way in which data protection principles are interpreted.

Consulting the Commissioner

229. In Chapter 7 we consider whether the Information Commissioner should have a right to be consulted on any legislation that involves surveillance or data powers, in order that he can communicate any concerns to Parliament. We now consider his involvement in the formation of government policy. The Commissioner told us that his approach was "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." (p 4) However, the ICO explained that it was often impossible for him to be involved in this way:

> "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 … At this stage it is often difficult to take

---

94 Data Sharing Review Report, op. cit., Recommendations 7(a) and 7(b), paras 8.30–8.31, 8.34.

95 ibid., para 8.34.

96 ibid., paras 8.35, 8.38.

97 Response to the Data Sharing Review Report, op. cit., pp 14–16.

> into account any privacy and data protection concerns that the Commissioner may raise. This can have the potential result of safeguards being implemented at a late stage as a compromise, and possibly more expensive, inadequate solution … In addition, the failure to consult with the Commissioner can have a detrimental impact on Parliamentary time, such as when the Serious Crime Bill was submitted to Parliament and subsequent amendments had to be made … a greater obligation to consult with the Commissioner at an early stage in the design and legislative process is essential." (pp 5, 19–20)

230. The Commissioner suggested that the Government's failure to consult him at a sufficiently early stage was due partly to his independent status—a requirement of the European Union Data Protection Directive 95/46/EC—which meant he was "out of the Whitehall loop". (Q 14) Dr Chris Pounder, then of Pinsent Masons, went further and told us, "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 (i.e. whether personal data should be processed) and often are not fully addressed in the implementation of policy (i.e. how to process personal data)." (p 281)

231. **We regret that the Government have often failed to consult the Information Commissioner at an early stage of policy development with privacy implications. We recommend that the Government instruct departments to consult the Information Commissioner at the earliest stages of policy development and that the Government should set out in the explanatory notes to bills how and when they consulted the Information Commissioner, and with what result.**

Audit and inspection powers

232. Some witnesses argued that the Commissioner needed more powers to carry out unannounced inspections of organisations to assess their compliance with the DPA. Although the Commissioner has the power to carry out audits under the Act, these audits can only be undertaken with the permission of the data controller for the organisation in question, with the result that it is difficult for the Commissioner's Office to work proactively or act as an effective deterrent against bad practice. Professor Martyn Thomas, independent consultant and representative of the UK Computing Research Committee (UKCRC), argued:

> "I believe that strengthening the Information Commissioner's Office so that he has more resources to enforce the Act would be extremely beneficial. Giving him the ability to require that audit activity be undertaken—requiring, for example, that a company's auditors reported on compliance with the Data Protection Act—that could be very powerful because it would extend the ICO's reach and it would provide an independent check on whether the DPA was being followed." (Q 378)

233. Dr Daniel Neyland, then Senior Research Fellow at the Saïd Business School, University of Oxford, called for "selective, random, unannounced inspections of state funded data management systems" by the Information Commissioner. (p 424) In addition, Dr Murakami Wood suggested that he should also be empowered to inspect private sector organisations because

"these vast new conglomerates of information … need to be subject to inspection as much as the state". (Q 68) Dr Eric Metcalfe, Human Rights Policy Director for JUSTICE, told us that it was a "basic anomaly" that the Commissioner could audit a private company but did not have the power to compel an audit. (Q 276)

234. The Commissioner was clear in his desire to have his current auditing powers increased (Q 8), telling us that the requirement to have the consent of the data controller before conducting an inspection "limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance." (pp 5–6) Deputy Information Commissioner David Smith put the situation into a broader context by suggesting that "we are, as far as we can see, almost unique as a regulator in having a set of responsibilities to oversee and not then having a power to inspect that they are being put into practice." (Q 19) The Commissioner argued that a power to carry out proactive inspections would, by contrast, "send a strong signal that compliance with the law is not just for the virtuous but needs to be taken seriously by all." (p 6) The House of Commons Home Affairs Committee reached a similar conclusion, calling for an extension of the Commissioner's inspection and audit powers.[98]

235. The Thomas-Walport Review considered this issue. It referred to the Republic of Ireland's Data Protection Act, which grants strong inspection powers, and to the concern that without such powers the UK might not be compliant with the European Data Protection Directive. It concluded that the Information Commissioner should have "a statutory power to gain entry to relevant premises to carry out an inspection, with a corresponding duty on the organisation to co-operate and supply any necessary information" and that "where entry or co-operation is refused, the Commissioner should be required to seek a court order", although not a search warrant.[99] The report also suggested that the right to carry out spot checks of public sector organisations should be placed on a statutory footing.[100]

236. In the wake of the data loss by Her Majesty's Revenue and Customs (HMRC), the Prime Minister authorised the Information Commissioner to spot check government departments.[101] The Government told us that the subsequent interim report of their review into *Data Handling Procedures in Government* "committed on extending the spot checks to the entire public sector". (p 324) The Government have now indicated that legislation for this is intended, giving the Commissioner inspection powers over public sector data controllers without consent.[102] This provision has been included in the Coroners and Justice Bill in the 2008–09 parliamentary session, but this does not extend the power to cover the private sector in circumstances where there is no reason to suspect non-compliance or a breach of data protection principles.[103]

---

98 *A Surveillance Society?*, op. cit., para 195.

99 Data Sharing Review Report, op. cit., paras 8.61–8.65.

100 ibid., para 7.9.

101 HC Deb 21 Nov 2007 col 1179.

102 Ministry of Justice, The Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998: Summary of Responses, November 2008, p 6.

103 ibid., pp 16–17.

237. In responding to the Ministry of Justice's announcement about the ICO's new public sector inspection power, David Smith stated that "we would have preferred to have this power to undertake audits extended to private sector organisations as well."[104] The Commissioner will still have to obtain the private sector data controller's consent or, if he has reasonable grounds for suspecting a contravention of the data protection principles or a breach of the DPA, a time-limited judicial warrant giving search and seizure powers.

238. **We welcome the Government's decision to provide a statutory basis for the Information Commissioner to carry out inspections without consent of public sector organisations which process personal information systems, but regret the decision not to legislate for a comparable power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide. In addition, the protection of citizens' data may in the absence of legislation be vitiated given the growing exchange of personal data between the public and private sectors.**

The Commissioner's power to levy penalties

239. The Information Commissioner lacks the power to punish individuals or organisations for breaching the provisions of the DPA. Instead, his power is limited to issuing enforcement notices in the event of non-compliance. Dr Pounder told us that:

> "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." (p 281)

240. The ICO told us:

> "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." (p 6)

241. Similarly, Toby Stevens, Director of the Enterprise Privacy Group, warned us that "the majority of organisations in the private sector, if they were to choose to do so, could disregard most of [the DPA's] requirements, knowing that the outcome will probably be cheaper than the cost of compliance." However, Mike Bradford, Experian's Director of Regulatory and Consumer Affairs, did remind us that "while the cost of non compliance in terms of censure may be potentially minimal, for a commercial organisation, especially a plc, to end up with a headline that says 'There has been a data

[104] ICO, *Statement*, 24 November 2008.

breach at Company X' is a phenomenal cost to the business … the deterrent is in the breach which will potentially be reported." In respect of the public sector, Toby Stevens said, there were often no penalties "where there is little point in transferring taxpayers' funds from one body to another in the form of a fine." (Q 329)

242. Since we received this evidence, the Commissioner's concerns have been addressed in the Criminal Justice and Immigration Act 2008. The Act empowers the Commissioner to impose monetary penalties on data controllers (in the public or private sector) for breaching the data protection principles knowingly or recklessly in ways that are serious and likely to cause substantial damage or distress; the penalty may be appealed to the Information Tribunal (section 144). However, the Commissioner's new power has not yet been brought into force, and the Secretary of State has not set the maximum penalty level. The Thomas-Walport Review called for the power to be brought into force by 8 November 2008[105] and for the penalties to "mirror the existing sanctions available to the Financial Services Authority" with "high, but proportionate" fines related to turnover.[106]

243. **We welcome the new powers for the Information Commissioner to levy fines on data controllers for deliberately or recklessly breaching the data protection principles, and we recommend that the Government bring these powers into force as soon as possible. The maximum level of penalties should mirror that available to comparable regulators, and should not be disproportionate. This must be subject to an appropriate appeals procedure.**

Resources

244. The new powers proposed above will have resource implications for the ICO. The ICO's data protection activities are funded by the £35 notification fee paid by data controllers, whilst its Freedom of Information activities are funded by the Ministry of Justice. Several witnesses felt that the ICO was under-funded. Toby Stevens told us that the ICO "is not adequately resourced to keep up with the legislative burden being placed upon it" and that it therefore has to remain focused on "promoting data protection awareness rather than enforcing data protection because that requires such a great resource intensiveness". (Q 329) The Information Commissioner confirmed that "our resources are very limited". (Q 15)

245. Although Dr Pounder acknowledged that the introduction of new powers would require the resources of the ICO to be substantially increased, he was of the view that this was not an unreasonable demand:

> "The Commissioner has to be given the resources to do the job. At the moment £10 million is the money that the Commissioner generates, not from public sources but from registration fees. This compares unfavourably with the hundreds of millions of pounds in the budget of the FSA [Financial Services Authority] or the Health and Safety Executive or even the Food Standards Agency." (Q 847)

246. The House of Commons Justice Committee highlighted "the anomaly that the same basic registration fee of £35 is paid by individuals, small businesses,

---

[105] That is, six months after the Act received Royal Assent.

[106] Data Sharing Review Report, op. cit., paras 8.52–8.53

large companies and large government departments or agencies" and suggested that "a graduated rate would be more appropriate, more likely to reflect actual costs, and more suited to providing an adequate income for the policing of data protection."[107] Echoing this recommendation, the Thomas-Walport Review concluded that "changes should be made to the notification fee through the introduction of a multi-tiered system to ensure that the regulator receives a significantly higher level of funding to carry out his statutory data-protection duties."[108] We are pleased that the Government have accepted this proposal.[109]

The RIPA commissioners

The regulatory structure

247. There are three commissioners with oversight duties under RIPA: the Chief Surveillance Commissioner, the Interception of Communications Commissioner and the Intelligence Services Commissioner.[110] The Association of Chief Police Officers (ACPO) did not believe that this regulatory structure is effective and appropriate, telling us that the commissioners "adopt different methodologies, have different styles and do not co-ordinate their inspection activities" and that the current arrangements are "inefficient, cause duplication and are anachronistic." (p 43) Assistant Chief Constable Nick Gargan, the former Chair of the Covert Investigation (Legislation and Guidance) Peer Review Group within ACPO, argued that the duplication had a "bureaucratic cost" because of the resources needed to prepare for inspections that often resulted in conflicting advice which confused staff. He said that the structure was "an irritation rather than a substantial problem" but that a combined inspectorate would be "an opportunity both for lessening the burden on police forces but also for improving the quality of regulation." (Q 132)

248. Gareth Crossman, the then Director of Policy at Liberty, also favoured creating a combined inspectorate to replace the three RIPA commissioners, arguing that the tripartite system was a pointless historical anomaly. He concluded that "we should get rid of the whole lot and have a single Commissioner responsible for the oversight of intrusive surveillance currently covered by RIPA." (Q 279)

249. The analysis of the current system given by Nick Gargan was disputed by the Interception of Communications Commissioner, Sir Paul Kennedy. Sir Paul contested the point about duplication on the grounds that "the activities being considered by the representatives of the Office of Surveillance Commissioners … and those being considered by the Inspectors from my office are different." He also disputed Nick Gargan's claims about clashing inspection visits and conflicting advice from different offices. (pp 62–63)

250. Nick Gargan explained that his comments on duplication reflect "a strongly held and often repeated viewpoint of many senior practitioners" and reiterated his view that a merged body could rationalise the inspection

---

[107] Protection of Private Data, op. cit., para 26.

[108] Data Sharing Review Report, op. cit., Recommendation 13, p 4. See also para 8.67.

[109] The Information Commissioner's Inspection Powers: Summary of Responses, op. cit., pp 19–20.

[110] There is also an Investigatory Powers Commissioner for Northern Ireland. See Box Two above for a description of the commissioners' responsibilities.

process. He repeated the point about conflicting advice and gave an example where Sir Paul Kennedy's office had given advice that contradicted guidance from the Office of Surveillance Commissioners (OSC). (pp 64–66) Subsequently, Assistant Chief Constable Suzette Davenport, his successor as Chair of the Peer Review Group, wrote to us on behalf of ACPO to underline the point that "there is much overlap between inspection regimes", and to assert that "greater clarity around the remit of each inspection regime can only be of benefit both in terms of efficiency and in avoiding any misunderstandings around role, function and remit." (pp 66–67)

251. The Chief Surveillance Commissioner, Sir Christopher Rose, argued against a merged inspectorate:

> "The answer to that is no, because the job has to be done. The areas which Sir Paul covers are entirely different from mine, and those processes have to be inspected by somebody, so if you had a single Commissioner responsible for everything, there would still have to be the same inspection carried out of the public authority or the law enforcement agency in relation to that particular sphere of activity. I would have thought, particularly in an area which is, partly as a result of the legislation and partly for practical reasons, quite technical and difficult, the more specialism you have among those who are keeping an eye on what goes on, the better the public interest is served." (Q 643)

252. **We are concerned that three different offices overseeing the operation of the Regulation of Investigatory Powers Act 2000 (RIPA) may result in inefficiencies and disjointed inspection. We recommend that the Government examine the feasibility of rationalising the inspection system and the activities of the three RIPA Commissioners.**

Quality of oversight

253. Sir Christopher Rose told us that law enforcement agencies were inspected every year by his Office while public authorities were inspected only "every two years or every three years". The inspection process consisted of "a dip sample of the paperwork" which led to a report which he then had to approve and, in the case of law enforcement agencies, a follow-up meeting with the Chief Constable. (Q 648) Sir Christopher accepted that this system had its limitations:

> "So far as my check on what goes on is concerned, as I said earlier, all we can do, we are a tiny outfit, is a dip sample … [but] if [the bodies under inspection] have chosen to do it improperly, without any paperwork, there will be nothing for us to inspect, but I have no reason to believe that any public authority would be foolish enough to embark on that sort of conduct … I cannot prove that [the dip sample] is adequate, because the 10 per cent of documentation, or whatever it is in the particular case, which is examined may or may not be representative, so I cannot prove that it is adequate." (QQ 652, 654)

254. Sir Paul Kennedy, as Interception of Communications Commissioner, operates by inspecting interception warrants issued by the Home Secretary and random samples of applications for communications data within law enforcement agencies and public authorities. He told us that such inspections needed to continue indefinitely but that compliant institutions would be inspected less frequently than non-compliant ones. (QQ 684, 706, 724)

255. This regime of inspections seems to be a proportionate and cost-effective way of examining the use of RIPA powers, and to be leading to a general improvement in the level of compliance.[111] However, the system does not provide any scope for targeted inspections in response to alleged abuses that may have caused public concern. For example, when it emerged that Poole Borough Council had used covert surveillance powers under RIPA to monitor a family to establish whether they lived in a particular school catchment area,[112] and later to monitor fishermen,[113] there was substantial public concern. The OSC, however, took no action and did not examine the use of the powers in these cases. The ICO did investigate, but the OSC only assessed the Council's conduct as part of its two-yearly inspection process.

256. When we asked Sir Christopher if he would consider investigating specific cases reported by the press such as those in Poole, he answered as follows:

> "Certainly not. It would be totally impossible to do that. As I say, there are a very large number of authorities which we inspect, we have a carefully designed programme. I mean, I am not ruling it out absolutely, if there was a well documented manifest abuse of power by a local authority, well then, of course we would try and do something about it, but I am afraid responding to press reports is not always a fruitful activity when you only have a small amount of resources at your disposal." (Q 653)

257. This answer is unsatisfactory. Whilst we understand that resources are constrained, it is essential that the regulators overseeing the use of RIPA powers should maintain public confidence in the regime. **We recommend that the Chief Surveillance Commissioner and the Interception of Communications Commissioner should introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner.**

The Investigatory Powers Tribunal

258. The Investigatory Powers Tribunal (IPT) is charged with investigating complaints against organisations, including the intelligence services, over their use of powers regulated by RIPA. The IPT also has jurisdiction over complaints brought by an individual concerning the acquisition, storage and use of information by the intelligence services of his or her entry in the National Identity Register established under the Identity Cards Act 2006. We note the concern expressed by Nick Gargan that "very few people" know about the IPT and that this represents a "missed opportunity" to demonstrate the transparency of the RIPA regime and to provide a visible means of redress for those who feel they have been wrongly treated. (Q 142)

---

[111] See for example the Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2007–2008, July 2008 (HC 659); and the Report of the Interception of Communications Commissioner for 2007, July 2008 (HC 947).

[112] Poole Borough Council "admitted using laws designed to track serious criminals to spy on a family for nearly three weeks to find out if they were lying about living in a school catchment area." Schlesinger F, "Council uses criminal law to spy on school place applicants", *The Guardian,* 11 April 2008.

[113] See for example Morris S, "Council used terror law to spy on fishermen", *The Guardian*, 14 May 2008.

He told us that "the tribunal ought to be encouraged to be a more publicly visible facility both in terms of encouraging people to use it and, where meaningful claims have been made, to actually publicise those findings so as to reassure the community that they are being protected and we are using our powers responsibly." (Q 144)

259. **We recommend that the Investigatory Powers Tribunal publicise its role, and make its existence and powers more widely known to the general public.**

CHAPTER 6: GOVERNMENT

Privacy protection in government: strengths

260. Successive governments have stressed the importance of protecting privacy and limiting the surveillance activities of the state. Most recently, in a speech in June 2008, the Prime Minister emphasised the need to preserve individual liberties when introducing new measures to fight crime and terrorism such as those relating to identity cards, the National DNA Database (NDNAD), and CCTV.[114]

261. Tony McNulty MP, the then Home Office Minister for Security, Counter-terrorism, Crime and Policing, told us:

> "As our democracy has developed we have struggled with the rights of the individual and privacy and that individual's responsibility, and the duty afforded to the state in terms of public protection and public welfare … the debate we are having now is about striking that balance, given other factors like … technology data and all the other elements. I would … weigh in that balance very strongly the rights of the individual and those broader rights of the state. Where there is a contest, other than in extreme cases, the rights of the individual prevail rather than the state; that is our democratic tradition and value." (Q 924)

262. His successor, Vernon Coaker MP, told us that "respect for human rights" is a core principle "with respect to all of the work that we do in this area. We have to cherish the right to privacy. That is fundamental to all of us and needs to be protected. The Government has always been clear that where surveillance or data protection impacts on privacy that should only be done where it is both necessary and proportionate … Of course, the other principle to balance up with all of that is the desire to protect the public … not only from terrorism but also from serious crime … It is about where we draw the line and how we have the correct balance between these things which is absolutely essential. It is not always easy to do that." (Q 1010)

263. Vernon Coaker also told us that "different times require the appropriate response to that particular time … Times change, technology changes. There are difficulties, there are threats to us, as we know only too well, which we have seen on our streets, and that requires us to take action against them. An important point is to say this: society should respond in the appropriate way to the threat that it faces at that particular time, always having regard to the need to balance national security with human rights, and the judgment of where that line should be drawn will vary from one age to the next." (Q 1071)

264. Michael Wills MP, Minister of State in the Ministry of Justice (MoJ) with responsibility for data handling issues, emphasised that:

> "It is important that this is not only about privacy, it is also about how we maximise the benefits of data sharing … I do not think we can ever look at these things in isolation. All of us often want two separate things at the same time. We are all very careful about our own privacy … However, we also want more efficient public services … you do need to

[114] Gordon Brown MP, Speech on Security and Liberty, *op. cit.*

> have data sharing. The question is how do you do that without, at the same time, compromising people's quite proper sense of their own privacy and confidentiality? That is the challenge." (Q 975)

265. The current Transformational Government agenda—an initiative aimed at transforming public services through the use of technology—includes an understanding that any new system of public service delivery should pay proper attention to the protection of privacy.[115] It also suggests that the maintenance of public trust should be treated as a requirement for any new public sector programme. Adherence to the principle of data minimisation—the collection or retention of the minimum amount of data necessary to carry out a designated function—is part of Transformational Government. Michael Wills interpreted this in terms of the integration of separate databases with a view to using data more efficiently rather than collecting less data. (Q 973)

266. The manner in which identities are verified in transactions plays a part in determining the extent of privacy protection. Government is aware that there are benefits to providing citizens with improved identity management.[116] Among these benefits is a reduced risk of identity fraud.

267. According to the Crosby report on *Challenges and Opportunities in Identity Assurance*, an identity assurance system (which differs from identity management by focusing on the interests of the consumer of services rather than on the interests of the owner of the database) shifts decisions on identification to the citizen:

> "The expression 'ID management' suggests data sharing and database consolidation, concepts which principally serve the interests of the owner of the database, for example the Government or the banks. Whereas we think of 'ID assurance' as a consumer-led concept, a process that meets an important consumer need without necessarily providing any spin-off benefits to the owner of any database. This distinction is fundamental … Some may wish to seek the potential benefits of 'joined-up government' and share their personal data across departments, if they are assured of the security of their data. Others will favour privacy over convenience and will prefer not to share any personal data. Ideally, ID assurance schemes should provide options".[117]

268. The Information Commissioner's Office (ICO) drew attention to the use in Austria of a system of identification numbers that allows access to information in different databases "without the need for a single widely known personal identification number that may be misused." (p 5) The Royal Academy of Engineering (RAE) explained that it is possible for individuals to fulfil their legitimate need or desire to maintain multiple roles or identities in transactions with state or other organisations and to avoid the possibility of those organisations needlessly correlating them. The technology involved in identification can be developed to suit an individual's preference to keep domestic status and work life separate, where the protection of identity is necessary to avoid abusive relationships or stalking, or where witnesses and children need protection.[118] **We recommend that the**

---

[115] Transformational Government—Enabled by Technology, op. cit., para 39(4); Cabinet Office, Transformational Government—Implementation Plan, March 2006, paras 53–58.

[116] Transformational Government—Implementation Plan, op. cit., paras 66–67.

[117] Sir James Crosby, *Challenges and Opportunities in Identity Assurance*, March 2008, p 3 and para 1.5.

[118] Dilemmas of Privacy and Surveillance: Challenges of Technological Change, op. cit., section 7.1.2.

Government's development of identification systems should give priority to citizen-oriented considerations.

269. The Department for Business, Enterprise and Regulatory Reform (BERR) told us:

> "It is the responsibility of each and every public authority to conduct any interaction with the public with legal care, consideration and a respect for fundamental human rights, particularly with regard to the collection, retention and sharing of personal data ... BERR takes the mantle and responsibility of public confidence very seriously, both understanding and acting to maintain the delicate balance between individual liberties and the safeguarding of the community in a democratic society." (pp 325–26)

270. Other Government departments also provided evidence of their efforts to protect privacy and work within the current human rights and regulatory frameworks. (pp 323–41)

271. In 2006, the Government established a Ministerial Committee, MISC 31, to develop a comprehensive data sharing policy for the public sector by Spring 2007. Although MISC 31 produced a "vision statement" on information sharing,[119] it never issued a final report and was eventually "overtaken by events". (Michael Wills MP, Q 974; and p 323) This coincided with the accession of Gordon Brown as Prime Minister, who, Michael Wills said, "felt there were real issues that needed to be addressed here … I think [MISC 31] did a valuable job in promoting collaboration. Some of the fruits of it we are still taking through". (Q 974)

272. Michael Wills and Belinda Crowe, Head of Information Rights Division at the MoJ, told us that the *Data Sharing Review Report*, by Richard Thomas, the Information Commissioner, and Mark Walport, Director of the Wellcome Trust (the Thomas-Walport Review), was by then considering some of the issues surrounding data sharing and privacy, and that the reviews of data losses[120] would play an important part in future thinking. (Q 974)

273. The work of MISC 31 has continued through inter-departmental activities. The MoJ explained that:

> "As part of the Service Transformation Plans, the MoJ will lead a cross-government programme to deliver a package of measures over the next three to five years to overcome the current barriers to information sharing within the public sector. The aim of this programme is to 'develop frameworks and mechanisms that enable public sector organisations to share information to improve personalised public services, increase public safety and tackle social exclusion in an environment of openness and respect for citizens' privacy and access rights'". (p 323)

274. The House of Commons Home Affairs Committee's report, *A Surveillance Society?*, recommended that "the principle of restricting the amount of information collected to that which is needed to provide a service should guide the design of any system which involves the collection and storage of

---

119 Information Sharing Vision Statement, op. cit.

120 Data Handling Procedures in Government: Final Report, op. cit.; Review of Information Security at HM Revenue and Customs, op. cit.; Report into the Loss of MOD Personal Data, op. cit.

personal information. We recommend that the Government adopt a principle of data minimisation in its policy and in the design of its systems."[121]

275. We recognise the need for data sharing across departments and agencies, but the principle of minimisation of data collection and processing must be rigorously observed. The Coroners and Justice Bill was introduced to the House of Commons on 14 January 2009 and contained proposals for extensive data sharing powers for the Government. We will pay particular attention to the parliamentary debates on this bill and conduct our usual bill scrutiny on it when it reaches this House.

276. In the course of developing the National Identity Card Scheme, the Government have sought to reassure the public that there will be appropriate safeguards in place to protect individual privacy. So far, however, a detailed description of these safeguards and how they will operate in practice has not emerged.[122] Central to the new scheme will be the use of biometrics. Fingerprints, iris patterns and facial recognition are forms of biometrics that are used in identification schemes. The independent Biometrics Assurance Group has commented on some inadequacies in the National Identity Scheme's system of identification and privacy protection, and on matters of consent and overall transparency. It has made recommendations for improvement in legal compliance, data sharing, and ensuring that cards and biometrics are compatible which have been accepted by the Identity and Passport Service.[123]

277. The Government have shown awareness of the need for privacy protection and the importance of maintaining public trust in other areas of surveillance and data use. The National DNA Database Ethics Group is responsible for maintaining a watching brief on broader issues.[124] The National CCTV Strategy has recommended that there should be better regulation of CCTV in the interests of privacy and data protection.[125]

278. We wrote to Vernon Coaker, asking for further information on the reported Government plans to create a centralised database which would keep a record of every electronic communication in the United Kingdom. His reply to us indicated that the Government was looking at ways of retaining communications data in the future but that this did not include recording the contents of the communications. (pp 361–62)

279. Vernon Coaker subsequently told us that "we are concerned about the way in which the capacity of law enforcement and the security services to access some of the data that they have been able to access is diminishing and we are concerned about some of the threats there are to that … the problem is that in a technological world where all of us are struggling to keep up the idea that all of the communications can be accessed now because somebody phones somebody else and the way in which it is changing through the internet is problematic for us. As a Government we have to take account of those changes in technology to ensure that our law enforcement and security services have the capacity to collect the information and data that they

---

121 A Surveillance Society?, op. cit., para 163.

122 See for example http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/how-the-data-will-be-used/

123 Biometrics Assurance Group, *Annual Report 2007*.

124 1st Annual Report of the Ethics Group: National DNA Database, op. cit.

125 National CCTV Strategy, op. cit., Chapter 3.

need". (Q 1041) He also stressed that "it is about maintaining our capacity, not about increasing it." (Q 1045)

280. He told us that the Government are "looking at the options that are available to us", with a public consultation document to follow in early 2009. (QQ 1041–42)

Privacy protection in government: addressing weaknesses

281. Tony McNulty told us of the Government's concern for privacy and awareness of the need for control over surveillance and the use of data. (Q 924) Recent data losses raise concerns about the way in which data security relates to data protection and human rights in the development of policies involving personal data.

282. The priority given to the rights of the individual over those of the state was commented on by Belinda Crowe:

> "When we looked at what the barriers to data sharing were in order to transform the way that public services are delivered, in actual fact data sharing and data protection was a small part of that and actually the main part was joining up together and different departments working together in order to deliver a particular policy outcome." (Q 974)

283. The Government have begun to act on many of the recommendations of recent critical reports on the storage and handling of personal data. If these recommendations were implemented effectively, they would eliminate many of the identified weaknesses of government as a controller of citizens' personal data and have a positive effect on citizen-state relations. But as yet there is little reason to doubt the critical observation made by the Joint Committee on Human Rights (JCHR) in its report, *Data Protection and Human Rights*, that "there is insufficient respect for the right to respect for personal data in the public sector."[126]

284. Michael Wills said that "a radical change of culture" was needed within Government about how they handle data: "That is the cultural challenge that all of us face—ministers, politicians and officials alike—and that is the challenge with which we are now grappling". (Q 972)

285. A succession of events have brought the Government to this conclusion.[127] Michael Wills agreed that, pending the recommendations of the recent reviews of data handling and data losses, "when you talk about privacy, there clearly is a role for some kind of formal mechanism for ministerial collaboration on these issues". (Q 975)

286. In the UK, the MoJ has departmental responsibility for data protection. During our visit to Canada, we learned that one of the responsibilities of the Canadian Department of Justice (DoJ) was to monitor developments in this field and to examine provisions for data sharing in different government departments. For example, lawyers from the DoJ actively worked inside other government departments, reporting back to the DoJ where necessary. In addition, the Canadian Minister of Justice has a statutory responsibility to certify that legislation is compatible with the Charter of Rights.[128]

---

[126] Data Protection and Human Rights, op. cit., p 3, and para 27.

[127] See Box One above.

[128] Appendix 4, para 4.

287. The JCHR has recommended enhancing the role of the data protection minister in this country, and giving the office a higher profile within government.[129] In response, the Government stated that departments were best placed to manage their own information, and that the cross-government Data Handling Review would show how co-ordination and learning would be carried out.[130]

288. The interim report of that Review emphasised solutions and new governmental roles—for example, departmental Senior Information Risk Owners—which relate mainly to information risk, security and assurance.[131] Whilst these are important issues, to concentrate on them may inhibit a more rounded consideration of privacy protection and the role of responsible ministerial leadership.

289. The Data Handling Review itself highlighted deficiencies not only in data security and protection, but also in civil service working culture and the understanding of the value of information. It expressed concerns about the responsibilities of chief executive officers and permanent secretaries for data handling, the standardisation of procedures, transparency, and performance scrutiny.[132] Among its specific recommendations were for Privacy Impact Assessment (PIA) (which we discuss in Chapter 6), better staff training and higher professional qualifications, risk assessment, and Cabinet Office responsibility for overseeing progress.[133] In an Annex, the Government asserted that the Cabinet Office was assisting in the promotion of cross-departmental learning.[134]

290. **We agree with the recommendation of the Joint Committee on Human Rights that the role of data protection minister should be enhanced and its profile elevated, and are disappointed that the Government's response has not grasped the main point about the need for more effective central leadership. The Government should report to the House through this Committee on the feasibility of having Ministry of Justice (MoJ) lawyers working in other departments and reporting to the MoJ on departmental policies with data protection implications, and of certification of legislative compatibility with the Human Rights Act 1998. This should be in conjunction with the current system of certification of compatibility by the Minister in charge of each bill going through Parliament.**

291. The Thomas-Walport Review identified inadequacies in the powers of the Information Commissioner to enforce the Data Protection Act 1998 (DPA), and sought to lift the "fog of ambiguity and uncertainty" caused by the complexity of the law and the plethora of guidance that inhibited legitimate data sharing.[135] The public sector was said to be lagging behind the private sector in the governance of information handling.[136] The Government have

---

129 Data Protection and Human Rights, op. cit., para 26.

130 Government Response to Data Protection and Human Rights, op. cit., pp 6–7.

131 Cabinet Office, Data Handling Procedures in Government: Interim Progress Report, December 2007, paras 7–12.

132 Data Handling Procedures in Government: Final Report, op. cit., paras 7–9 and Section 2.

133 ibid., Section 2.

134 ibid., Annex I.

135 Data Sharing Review Report, op. cit., Foreword, Chapter 7, and paras 5.21, 5.26, 5.30, 8.28.

136 Data Sharing Review Report, op. cit., paras 1.4, 5.28–5.29, 8.3–8.4

investigated serious lapses in data security, and implemented many of the recommendations of the Thomas-Walport Review. Government departments were taking remedial action before the Data Handling Review was published.[137]

292. The Thomas-Walport Review identified a need to improve decision-making about data sharing, to improve transparency and training, to use technology better to protect privacy, and to introduce other reforms in organisational culture and processes. **We support the recommendations made in the Thomas-Walport *Data Sharing Review Report* for changes in organisational cultures, leadership, accountability, transparency, training and awareness, and welcome the Government's acceptance of them. We urge the Government to report on their progress to Parliament.**

Privacy Impact Assessment and risk

293. There is also a need to respond to risk more effectively, and to increase public understanding of the risks involved in government and private sector information practices. The Coleman Report on *Protecting Government Information* examined the dangers of fraud, accidental damage and loss of data, espionage, cyber attack, and insider threats.[138] The Report recommended new processes and structures to deal with these risks, together with independent oversight and the introduction of Privacy Impact Assessments (PIAs).[139] The Government have accepted the main thrust of the Coleman Report's recommendations.[140]

294. Professor Angela Sasse, of University College London, and representative of the UK Computing Research Committee (UKCRC), told us:

> "The key problem is really that our ability to assess risks associated with information technology with electronic data has not kept up … The people who are handling the amounts of data, because they are in contact with them every day, are utterly blasé about the risks associated with the data and the value and they have no understanding … about the impact that that disclosure or leaking of those data has on the lives of the individuals who are affected by this leakage. Given that it is Government handling their own citizens' data, that is something that has to change. The Government have a duty of care." (Q 381)

295. The assessment of risk is central to the idea of PIAs, which are defined as "structured assessments of a project's potential impact on privacy, carried out at an early stage."[141] The Government currently advise that PIAs should be undertaken in the early stages of any policy implementation where information technology and systems are being developed for the purpose of data processing and surveillance. The Information Commissioner, Richard Thomas, told us that a number of foreign jurisdictions—notably Australia, Canada, New Zealand, and the United States—have introduced mandatory

---

137 Data Handling Procedures in Government: Final Report, op. cit.

138 Protecting Government Information—Independent Review of Government Information Assurance (The Coleman Report), June 2008, Chapter 3.

139 ibid. See especially p 7.

140 Data Handling Procedures in Government: Final Report, op. cit., pp 39–40.

141 Data Sharing Review Report, op. cit., para 5.5.

PIA systems, and require that all government departments produce and publish a PIA before any new information gathering or processing system is introduced. (p 5)[142]

296. Many of our witnesses supported the implementation of PIA. The Commissioner has strongly promoted PIA and in 2007 his office produced a handbook of materials on PIA procedures.[143] He told us:

> "It requires any major initiative, which is going to collect and use personal information, to go through a checklist … showing how they have identified the risks, they have minimised the intrusion and they have put safeguards in place." (Q 29)

297. Jonathan Bamford, Assistant Information Commissioner, told us:

> "The vision is based on other jurisdictions where it tends to be public authorities who are actually engaging in the use of information that applies to lots of people, used for potentially sensitive purposes like health. Obvious examples … would be ones like ID cards … Connecting for Health and the wider use of patients' information beyond their own surgeries." (Q 31)

298. The ICO told us that one major benefit is that the assessment process can take place "during the development of proposals when there is still an opportunity to influence the proposal." In addition, by requiring PIAs to be undertaken by a third party independent of the organisation introducing the new measure, the system can provide a measure of external validation. (p 5)

299. Professor Sasse told us:

> "I believe that if that were done competently and honestly, it would lead to much better protection and it would lead to less off-the-cuff decisions about what data to collect and how long to keep them for. If it is done competently and honestly, it also has a big pedagogical effect on the people in a company, so they learn how to do things better, they learn what to care about." (Q 408)

300. Dr Victoria Williams, a member of the Bar who has made a special study of PIA,[144] agreed that "PIAs, properly done, can impose that degree of mental discipline in analysing the potential impact of the surveillance programme. It requires the proposal to be broken down and considered analytically and made public … It also lays bare the internal workings of the scheme so that then whatever regulatory regime is in place can bite into those stages." She also suggested that PIA "might provide a framework for incorporating notions of how mass surveillance might affect society as well as simply data protection issues for the individual." (Q 592)

301. PIA could become an effective means of monitoring the effect technology such as public area CCTV may have on society as a whole. According to Dr Williams, the question of whether PIA could be adapted to systems of public area surveillance would depend on establishing through a constitutional review that a social impact was involved, and that the constitutional rights of free speech and assembly needed reinforced protections. (pp 210–11)

---

142 See also A Report on the Surveillance Society, op. cit., sections 45.1–45.2.

143 See http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

144 Williams V, "Privacy Impact Assessment and Public Space Surveillance", 2007.

302. Witnesses drew our attention to the dangers of implementing PIA but then failing to take account of the assessments. Dr Williams expressed concern over the possibility of PIA becoming a perfunctory bureaucratic exercise. (Q 592) In order to avoid the "risk [of PIA] becoming mere paperwork", she contended that "surveillance" PIA should be published, reviewed, approved by a competent authority, and linked to planning, regulatory, or funding decisions. (p 210) Under the E-Government Act of 2002, most of these conditions are imposed on agencies in the USA federal public sector.

303. Officials at the US Department of Homeland Security (DHS) argued that PIA was a useful technique because it forced the DHS to think very carefully about privacy and how to build in privacy safeguards. The system had "teeth" because PIAs in the USA were linked to funding. In addition, the officials believed that PIAs should be made public so as to improve awareness of Government surveillance activities, and raise levels of public confidence and trust.[145]

304. Members of the Center for Democracy and Technology in Washington, DC told us that PIAs varied considerably in quality. They suggested that some, such as those used for the new passport system, were little more than mere "box-ticking" exercises. We were told that the US Government is seeking to develop and disseminate best practice. Nonetheless, members of the Center thought that if departments were determined to press ahead with particular schemes, it was unlikely that PIAs could make much difference.[146]

305. Dr Gus Hosein, Senior Fellow at Privacy International, and Visiting Senior Fellow at the London School of Economics (LSE), told us that it would be "a highly recommended step forward" for the UK Government to be required to undertake PIAs. However he warned that it was possible that a highly privacy-invasive scheme might pass a PIA test, as he claimed was the case with the US-VISIT programme that takes and stores the fingerprints of all foreign visitors to the United States. (Q 245) Dr Williams drew our attention to the FBI's PIA for their DNA database, a document which "ticks all the boxes and … complies with all the criteria" but was not informative. (Q 592)

306. We welcome the commitment in the Government's Data Handling Review to adopt PIA across all departments.[147] PIA is now also adopted in identity management programmes.[148] The Thomas-Walport Review saw PIA as a way "to make clear the thinking behind a proposed data-sharing scheme and to demonstrate how the questions of proportionality are being addressed."[149] The Review recommended that any draft order laid by a Secretary of State to remove or modify a legal barrier to data sharing must be accompanied by a "full and detailed" PIA that would "assist both the Information Commissioner and Parliament's consideration."[150] The Government's response to the Review accepted the requirement of a mandatory PIA in such circumstances, but appeared to outline a version of a PIA that would also emphasise "benefits for individuals and the general public" of a proposed

---

145 Appendix 4, para 77.

146 ibid., paras 50–51.

147 Data Handling Procedures in Government: Final Report, op cit., para 2.11.

148 ibid., p 40.

149 Data Sharing Review Report, op. cit., para 5.5.

150 ibid., para 8.43.

data sharing initiative.[151] We would be concerned if the main purpose of a PIA were to reflect such emphases, or if PIAs were not conducted sufficiently early in the policy process.

307. **We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs. We also recommend that the Government—after public consultation—consider introducing a similar system for the private sector.**

Necessity and proportionality

308. In order to comply with the Human Rights Act 1998 (HRA) and Article 8 of the European Convention on Human Rights (ECHR), organisations engaged in surveillance and data collection must ensure that such activities are both necessary and proportionate.

309. Professor Graeme Laurie of the University of Edinburgh Law School, who contributed to the Nuffield Council on Bioethics' report on *The forensic use of bioinformation: ethical issues*, told us that the starting point for that report was:

> "The fact that we have fundamental rights of liberty, privacy and autonomy … If we wish to move from that then the obligation and the onus is on the state to show that it is necessary and proportionate in particular circumstances, and the circumstances obviously depend on what are the social ends that you are trying to achieve". (Q 169)

310. Gareth Crossman, the then Director of Policy at Liberty, went further:

> "The question of proportionality is very important. Legitimate state interference into individual privacy is, of course, part and parcel of a democratic society, but as a consequence of a number of factors over the last few years, the concept of proportionality … the need to only do things in a way which is appropriate to the situation faced, has fallen away from surveillance, whether it be mass surveillance through a database, whether it be through visual surveillance of CCTV or targeted surveillance through the use of the Regulation of Investigatory Powers Act, so underpinning our concerns over surveillance is that the accountability and proportionality elements have fallen away." (Q 221)

311. Dr Eric Metcalfe, Human Rights Policy Director for JUSTICE, suggested that Parliament might restrain the executive's enthusiasm for surveillance by "refusing to pass disproportionate laws" and by scrutinising laws "very closely in terms of their proportionality and, going back to the basic point, the necessity. Is it actually necessary, for example, to create a national identity card?" (Q 248)

312. Peter Hustinx, the European Data Protection Supervisor, raised a related concern about necessity in the context of counter-terrorism and security in Europe:

---

[151] Response to the Data Sharing Review Report, op. cit., p 17.

> "We see it all the time: measures are being piled up and they are not being evaluated. Sometimes there is an overdrive: 'This is important; we cannot wait; we need to do this now', and the overdrive is the moment where risks are taken without sufficient evaluation because there is a perceived need to do something." (Q 479)

313. In his view, the proposal for the European Passenger Name Record[152] failed to provide much evidence of necessity and proportionality except vaguely and anecdotally. (Q 481) Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), thought that Article 8 of the ECHR, which guarantees a right to privacy with certain restrictions, was too easily overridden by governments' unsubstantiated assertions about the necessity of, for example, an anti-crime measure. (Q 492)

314. On the other hand, we were told by David Feldman, Rouse Ball Professor of English Law, University of Cambridge, that the test of necessity "requires that the interfering authority must show that the interference serves a legitimate aim, and that is not too difficult a job to meet." (Q 520) However:

> "A proportionality requirement … can be a substantial burden on a justifying agency, but whether it is a really robust protection depends on how effectively the reviewing body applies the proportionality test and also how carefully the body which has to authorise the interference in the first place applies it. If it works well, it can be a very effective protection indeed … If one were to adopt … a more deferential view to the question of proportionality and treat with considerable respect the view of the original decision-maker as to whether the interference was justified and proportionate, that would be a much less useful protection." (Q 520)

315. Sir Christopher Rose, the Chief Surveillance Commissioner, whose staff scrutinise the decisions of officers who authorise surveillance, commented on how the proportionality of surveillance was determined:

> "The methods used have to be proportionate to what is sought to be achieved, and so authorising officers, whether of law enforcement agencies or other public authorities … have to balance the intrusiveness of the activity against the operational need, and that is something which can be found in the Code of Practice." (Q 664)

316. Sir Paul Kennedy, the Interception of Communications Commissioner, saw necessity and proportionality as offering protection to the citizen. (Q 721) His inspectors found that, in almost all cases, the application for communications data was justified. (Q 716) However, Sir Paul accepted the need for periodic inspections because of the possible slippage in standards. (Q 724) He also considered that the training for police offered under the auspices of the West Mercia Police Force had contributed to great improvements. (Q 708) The Home Office, the Association of Chief Police Officers (ACPO) and the Local Authority Coordinators of Regulatory Services (LACORS) ensure that local authority authorising officers receive legal and human rights training with respect to surveillance. The training is

---

[152] A Passenger Name Record (PNR) holds many details about a passenger, including name, age, details of contact, ticketing and payment, frequent flyer details, special meals or personal assistance needs, passport details, itinerary, etc.

designed "to ensure they have a thorough understanding of necessity, proportionality, privacy issues, collateral intrusion, etc."[153]

317. Sir Christopher Rose described the human rights element of the training received by authorising officers for making these judgments. (Q 666) He told us that law enforcement authorities were much closer to achieving a uniform standard of compliance than were "some public authorities" (Q 651):

> "So far as the law enforcement agencies are concerned, all of them, I think I can say now, with no obvious exception, take seriously their responsibilities to act essentially in a human rights compliant way … and they have gone to considerable lengths to provide the training so that their officers who are doing this job know exactly what they are doing … Other public authorities I am less confident about." (Q 655)

318. The Chief Surveillance Commissioner's 2007 Annual Report was more explicitly critical on this point:

> "[Government departments and local authorities] tend to resort to covert activity as a last resort but, when they do, have a tendency to expose lack of understanding of the legislation by completing documentation poorly. In particular there is a serious misunderstanding of the concept of proportionality. It is not acceptable, for example, to judge, that because directed surveillance is being conducted from a public place, this automatically renders the activity overt or to assert that an activity is proportionate because it is the only way to further an investigation."[154]

319. Such criticism is serious, as is demonstrated by recent reports of local authority covert surveillance, which we reflected on in Chapter 4. Training personnel, and helping them better to understand the meaning of necessity and proportionality in the context of the Regulation of Investigatory Powers Act 2000 (RIPA), appears to be a crucial element in helping to safeguard the citizen against excessive surveillance. Inadequate and inconsistent training in organisations permitted to engage in surveillance is likely to have detrimental effects on public trust, and to lead to concern about the possibility of the state's infringing people's legitimate expectation of privacy.

320. Codes of Practice can play an important role in guiding decisions on necessity and proportionality. Several Codes of Practices are in force under RIPA.[155] Both Sir Christopher (Q 664) and Sir Paul (Q 724) referred to Codes when telling us about the application of the tests in their respective areas of responsibility. The Codes give extensive and detailed guidance on the determination of necessity and proportionality, and on the importance of making correct determinations for the protection of human rights. The work of the Commissioners' inspectors involves establishing that authorisations have complied with legislation and with the Codes.

---

[153] LACORS Parliamentary Briefing Document on the Draft Consolidating Orders on the Regulation of Investigatory Powers Act 2000 (RIPA), June 2008, pp 4–5.

[154] Annual Report of the Chief Surveillance Commissioner, op. cit., para 9.2.

[155] Covert Surveillance—Code of Practice, op. cit.; Home Office, Acquisition and Disclosure of Communications Data—Code of Practice, 2007; Home Office, Investigation of Protected Electronic Information—Code of Practice, 2007; Home Office, Covert Human Intelligence Sources—Code of Practice, 2002; Home Office, Interception of Communications—Code of Practice, 2002.

321. Sir Paul Kennedy's Annual Report for 2007 indicated the central importance of the Code of Practice in regulating communications surveillance practices. The Report remarked that local authorities' specialist staff who were involved in applications for communications did not receive training to the same standard as in other public authorities, and that this had resulted in a lower level of compliance with the Code of Practice.[156] For the year ahead, Sir Christopher Rose's Annual Report for 2007–2008 welcomed without further clarification "the intention to identify and amend those elements of the legislation or Codes of Practice that, in the light of experience, are unnecessarily inhibiting operational effectiveness."[157]

322. We would be concerned if the application of the Code were to be substantially softened in order to facilitate surveillance operations. The Codes do not, by themselves, instruct authorising officers how to interpret the criteria in individual cases and to determine whether a particular measure is both necessary and proportionate.

323. **We recommend that the Government devote more resources to the training of individuals exercising statutory surveillance powers under the Regulation of Investigatory Powers Act 2000, with a view to improving the standard of practice and respect for privacy. We recommend that the principles of necessity and proportionality are publicly described and that the application of these principles to surveillance should be consistent across government.**

The limits of legal regulation

324. We do not believe that the Government should confine themselves to questions of legal authorisation and compliance when seeking to improve surveillance practices. Although proper legal regulation is clearly necessary and important, we believe that the law alone cannot prevent individuals and institutions from abusing their surveillance powers. We agree with the JCHR that concentrating on legal responses is unlikely to generate the required level of commitment to human rights or concern for privacy amongst public sector staff.[158]

325. In addition, ensuring compliance with the law may not lead to an increase in public trust and confidence. Surveillance and data handling practices that are perfectly legal may nonetheless be undesirable according to other broader ethical or constitutional criteria. This may be particularly true where the legal rules are based on primary or secondary legislation that has not been sufficiently scrutinised by Parliament. We discuss such issues in Chapter 7.

Technological safeguards: strengths

326. "Privacy-enhancing technologies" (PETs) are technological safeguards that form part of the design of systems that gather and process personal information. PETs are central to the idea of "privacy by design",[159] which

---

156 Report of the Interception of Communications Commissioner, op. cit., para 3.25.

157 Annual Report of the Chief Surveillance Commissioner, op. cit., para 11.1.

158 Data Protection and Human Rights, op. cit., para 21.

159 This seeks to ensure that organisations give due consideration to data protection prior to the development of new initiatives. See Enterprise Privacy Group, *Privacy by Design—An Overview of Privacy Enhancing Technologies*, November 2008.

suggests that privacy is best protected by a comprehensive strategy that embraces organisational, technical, and legal responses to the challenge of surveillance. If PETs are effective, they reduce the need for individuals to rely on the law and formal regulations in order to protect their privacy.

327. The main assumption behind PETs is that design solutions can directly and reliably reduce the dangers associated with certain surveillance and data processing technology. The design of software may, for example, allow or prohibit certain operations that involve the collection of personal data. Information system architecture and the default rules which are built into the design of such systems can be more, or less, protective of privacy, depending on the decisions that lie behind their design and implementation.[160]

328. The Information Commissioner, who actively promotes "privacy by design", has published guidance material explaining and encouraging the use of PETs, and highlighting how they can give people greater control over their information and how it is used.[161] His response to the Government's consultation on Transformational Government focused on their importance.[162] Jonathan Bamford expressed the hope that those developing technology would seek to "look at privacy friendly ways of using that technology." (Q 27)

329. David Smith, Deputy Information Commissioner, told the House of Commons Justice Committee:

> "Data minimisation … is absolutely key to data protection and, when we are talking about these technological approaches, we are not just talking about security, we want a technological approach to the whole of data protection, what we term privacy enhancing technology: building in compliance, data minimisation, checks on accuracy, all part of the system".[163]

330. Data encryption is an example of a PET currently used by many public and private sector organisations. Jonathan Bamford noted that the use of encryption in laptops is a relatively simple and cost-effective privacy protection. (Q 27) However, the encryption policies and practices of Her Majesty's Revenue and Customs (HMRC), including the failure to use appropriate levels of encryption when dealing with highly sensitive personal data, were heavily criticised in Kieran Poynter's *Review of Information Security at HM Revenue and Customs*.[164]

331. The effectiveness of encryption tools will vary according to the competence of the people using them and their awareness of the importance of individual privacy. A number of reports have highlighted serious shortcomings in the approach taken to encryption in the public sector in recent years. **We believe that encryption has a vital role to play in ensuring the security of**

---

[160] See Lessig L, *Code and Other Laws of Cyberspace*, 1999; Reidenberg J, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, Vol 76, No. 3 (February 1998), pp 553–93.

[161] Information Commissioner's Office, Data Protection Guidance Note: Privacy Enhancing Technologies (PETs), March 2007; and Information Commissioner's Office, Privacy by Design Report Recommendations: ICO Implementation Plan, November 2008.

[162] Information Commissioner's Office, Information Commissioner's Response to the Cabinet Office Consultation on 'Transformational Government: Enabled by Technology', February 2006, pp 4–5.

[163] Protection of Private Data, op. cit., Oral Evidence, Q 40.

[164] Review of Information Security at HM Revenue and Customs, op. cit.

data, and that the Government should insist upon its use as appropriate throughout the public and private sectors.

332. Authentication and identification systems provide another means by which privacy can be protected through design. Increasingly, people are being asked to identify themselves or to "show ID" in situations where previously identification would have been considered unnecessary. Often, however, all that is actually required is verification of entitlement—for example, to receive a service or benefit, or to gain access to premises—and there is no obvious need for individuals to disclose their personal details. Systems can be designed to provide services on an anonymous basis, rather than requiring personal details to be revealed every time someone's claim for a service or benefit needs to be verified.

333. As the RAE has shown, identification and verification systems can be designed with a view to providing individuals with a significant amount of control over the disclosure of their personal information.[165] The RAE report observed that phone or travel cards are good examples of technology that enables payments to be made anonymously. Other forms of card can be developed that can, for example, be used to provide access to premises, or for the purposes of international travel, which do not divulge the identity of the card holder, but where the encrypted identification data can be accessed for legitimate reasons by law enforcement authorities.[166] However, NO2ID argued that the identity card scheme had "consistently blurred the distinction between authentication and identification, as if it doesn't matter." (p 427)

334. The ability to connect information systems and databases operated by separate organisations raises the question of how far privacy can be protected in the face of the Government's commitment to Transformational Government and greater data sharing in the public sector. The Home Office has said, for example, that under the National Identity Scheme:

> "The NIR [National Identity Register] will not be a single, large database. The sets of information—biometric, biographical and administrative—do not all need to be held in a single system. To help safeguard information and make best use of the strengths of existing systems, it makes sense to store them separately."[167]

335. However, where separate systems are merged into one database, security may be improved through policies and designs aimed at ensuring the separation of the identity documents associated with these systems. But whether databases of personal details are held separately but are accessible through technical and organisational procedures, or combined into one large collection, technical safeguards can play an important part in providing security as well as in privacy protection.

336. Following the repeated loss of personal information by various departments, the Government have argued that better handling of data will require a host of information security measures to be implemented commonly across the state. These include encryption where necessary, secure storage, access and

---

165 Dilemmas of Privacy and Surveillance: Challenges of Technological Change, op. cit., Chapter 7.

166 ibid., pp 37–38.

167 Home Office, National Identity Scheme: Delivery Plan 2008, p 25.

transfer, minimisation of the amount of information transferred by disc or laptop, and the logging and monitoring of use.[168]

337. **We welcome the Government's plans for better data handling. We recommend that the Government's report on progress on data handling and security be scrutinised by parliamentary committees.**

The limits of technological solutions

338. The limits of PETs are still being explored and debated by information specialists and lawyers. The RAE report said that whilst it was "not possible to guard against all conceivable ways of invading privacy … it is possible to 'design out' unnecessary compromises of privacy."[169]

339. Technological solutions, if not pursued within a wider design framework, may help to limit surveillance and protect privacy, but they should not be seen as a stand-alone solution. This is because the specific rules, norms and values—for example, data minimisation, access controls, and the means of anonymity—that may be built into technological systems must come from outside those systems themselves. We believe it is important to avoid assuming that a "technological fix" or "silver bullet" can be applied to what are essentially social and human rights issues.

340. Professor Martyn Thomas, independent consultant and representative of the UKCRC, told us:

> "There is a fundamental weakness at the heart of the transformational government agenda which is that you cannot build large databases that are accessible to a wide number of people and maintain a high degree of security … it is very difficult to build a database that is technically secure on top of commercially available, off-the-shelf software components, because almost all of them were not designed to support such a use, and to connect such a database to the internet simply creates a honey pot that virtually guarantees that the data will be extracted from it in a way that was not planned for or intended." (Q 407)

341. He pointed to a specific obstacle in the way of better security protection for personal data:

> "There is guidance in the Manual of Protective Security on how to carry out impact assessments on what the likely impact is of loss of personal data and on how such data should be protected. That manual is classified. As a consequence, it has not been peer-reviewed because it is only available to people whom government departments believe have a need to inspect it … I would expect that that peer review would lead to significant strengthening of the protection that was required of personal data because it would be seen to be clearly inadequate." (Q 407)

342. **In the interests of strengthening the protection of personal data, we urge the Government to make the Manual of Protective Security subject to regular and rigorous peer review.**

343. Going beyond the application of technological remedies, Professor Thomas outlined what needs to be done if privacy is to be taken seriously:

---

[168] Data Handling Procedures in Government: Final Report, op. cit., pp 16–18.

[169] Dilemmas of Privacy and Surveillance: Challenges of Technological Change, op. cit., p 37.

> "It requires proper hazard analysis … and then an appropriate set of protections to be put in place to address each of the hazards … It means using the appropriate technical … [and] social means to ensure that, firstly, you have understood the level of privacy that you are seeking, what level of breaches of confidentiality do you regard as tolerable … that you actually build the business processes, the social systems, the training and the technology to deliver that level of confidentiality in the systems … At the moment, that analysis appears not to be being done. There is no technical barrier to it being done, but it would lead to a lot of systems turning out to be a lot more expensive or not practical." (Q 416)

344. The importance of improving the technological safeguards for privacy has been underscored by the Council for Science and Technology (CST) in their plea for further research into PETs, including techniques for anonymising data, encryption, and countering viruses.[170]

345. **In the light of the potential threat to public confidence and individual privacy, we recommend that the Government should improve the safeguards and restrictions placed on surveillance and data handling.**

346. Toby Stevens, Director of the Enterprise Privacy Group, outlined current developments in industry regarding privacy technology:

> "The industry is focused very hard on this. The problem that they often seem to stumble up against is the lack of a common framework, a common language, a common understanding of what the problems are and what the desired outcomes look like … To date, most of the privacy-enhancing technology programmes that we have seen over recent years have failed, either due to lack of interoperability between those that roll them out or a lack of perceived consumer demand. That does not mean it is not there, but the consumers have failed to understand what it is they are being offered." (Q 297)

347. This situation is likely to inhibit government procurement of privacy-enhancing technology which, in the view of Philip Virgo, Secretary General of EURIM (the European Information Society Group), is already compromised by the life-cycle of the procurement process and the effect of the "churn" of ministers and officials on project specifications. (Q 303) Toby Stevens also thought that "government procurement does not reflect good privacy practice in general." (Q 303)

348. As the state is the main single "customer", public sector procurement specifications have an important influence on system design. The CST suggested that government, as the major procurer of information technology services and systems, should use procurement specifications to effect improvements in security.[171] In order for this to happen, as Professor Sasse told us:

> "It is the people who are commissioning and paying for the system who should have to be clear about what their security requirements are. Ultimately, the company who is building the thing will only give the customer what they ask for. They may raise a few points but currently

---

[170] Council for Science and Technology, *Better Use of Personal Information: Opportunities and Risks*, November 2005, paras 40–47.

[171] ibid., para 44.

we really have a problem that the customers often do not articulate their security requirements, they do not think about them." (Q 415)

349. **We recommend that the Government review their procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems.**

CHAPTER 7: PARLIAMENT

Introduction

350. In this chapter we consider the role that Parliament plays in surveillance policy.

351. Whilst the courts can declare primary legislation incompatible with the Human Rights Act 1998 (HRA) or strike down secondary legislation in certain circumstances, only Parliament can block legislation. Legislation may be rejected on the grounds that it breaches one or more of the key principles examined earlier in this report, such as the principle of executive self-restraint. As Dr Eric Metcalfe of JUSTICE told us, "it is for Parliament to decide ultimately what laws are made, and to scrutinise those laws very closely in terms of their proportionality and, going back to the basic point, the necessity." (Q 248) The barrister Dr Victoria Williams also emphasised Parliament's role: "In terms of where society draws the line in terms of how much we wish to be watched, it is a matter for the people at large, but of course Parliament is the voice of the people." (Q 605) This safeguard can only be truly effective if government places its surveillance and data schemes in a firm legislative framework.

Primary legislation

352. If Parliament is to scrutinise new government surveillance and data processing initiatives effectively, a sufficient level of detail must be given in primary legislation so that individual provisions can be properly debated and amended where appropriate. A number of witnesses warned that too many bills did not contain that necessary level of detail. For example, Action on Rights for Children (ARCH) commented that "it is unusual to find any power that governs surveillance clearly set out on the face of a Bill", highlighting in particular the Children Act 2004, which "resembled a blank cheque in that it contained a series of provisions for the Secretary of State to prescribe the content and governance of children's databases in regulations. It was only after intense lobbying and parliamentary pressure that the data items were specified on the face of the Bill and agreement reached that regulations would be subject to affirmative resolution." (p 271) Terri Dowty, Director of ARCH, warned us that "we are shifting our legislation to the Executive, effectively, in relying so heavily on secondary legislation, and I think there needs to be greater scrutiny." (Q 832)

353. Several witnesses focused on what they saw as the excessive delegation of powers in the Identity Cards Act 2006. The LSE Identity Project, which conducted extensive research on the introduction of ID cards, commented that "throughout the parliamentary debate about the Identity Cards Act, Home Office Ministers emphasized the fact that the Bill was 'enabling legislation' that would 'allow' a system of identity cards to be introduced." They quoted the minister then responsible, Tony McNulty MP, as saying that "there is much still to be done in terms of detail, regulations and all the other elements."[172] They added, "many of the details of the Scheme are not included in the Act, with these details being left to secondary legislation".

[172] HC Deb 28 June 2005 col 1253.

The Project's evidence concluded that this Committee should "look again at the role of 'enabling legislation' for legislation with such a profound impact on the relationship between the individual and the State, as there is a strong argument for not leaving the detailed implementation of the Act to secondary legislation". (p 414)

354. However, Tony McNulty insisted that the Act had been drawn more tightly than the other witnesses suggested. In a letter to this Committee, he noted that there were some 74 order-making powers in the Act, but that each order "must comply with sections one to three of the Act which clearly define the statutory purpose of the National Identity Register and the information that it may hold." (p 352) In spite of these reassuring words, we note that the statutory purposes of the Act are drawn in broad and flexible terms, such as "for the purpose of securing the efficient and effective provision of public services."[173]

355. In more general terms, Tony McNulty accepted "the premise that at least very, very clearly the principle and as much as possible the explicit functions and criteria for any data should be on the face of a bill", although he warned that "if you go in for undue specificity in terms of expressing things on the face of the bill, you sometimes cause more problems than leaving things more general." (Q 931) In relation to both the Identity Cards Act and other relevant statutes, the Minister insisted that "there are significant statutory safeguards in place which hold the order making process in check both in compliance with requirements set out in primary legislation and, importantly, by virtue of approval of each House of Parliament." The Government, he said, would "continue to adopt that approach." (p 352) We consider the implications of this approach for the Act's National Identity Register (NIR) later in this chapter.

356. The Joint Committee on Human Rights (JCHR) identified and criticised the trend described above, in respect of data sharing:

> "We fundamentally disagree with the Government's approach to data sharing legislation, which is to include very broad enabling provisions in primary legislation and to leave the data protection safeguards to be set out later in secondary legislation. Where there is a demonstrable need to legislate to permit data sharing between public sector bodies, or between public and private sector bodies, the Government's intentions should be set out clearly in primary legislation. This would enable Parliament to scrutinise the Government's proposals more effectively and, bearing in mind that secondary legislation cannot usually be amended, would increase the opportunity for Parliament to hold the executive to account."[174]

357. **We are concerned that primary legislation in the fields of surveillance and data processing all too often does not contain sufficient detail and specificity to allow Parliament to scrutinise the proposed measures effectively. We support the conclusion of the Joint Committee on Human Rights that the Government's powers should be set out in primary legislation, and we urge the Government to ensure that this**

---

173 Identity Cards Act 2006, Section 1(4)(e).

174 Data Protection and Human Rights, op. cit., para 20.

happens in future. We will keep this matter under close review in the course of our bill scrutiny activities.

Secondary legislation

358. No matter how much detail the Government puts into primary legislation in this field, some order-making powers will still need to be delegated to ministers in order to maintain a sensible level of flexibility without resorting to continuous amendment. In such cases, it is important that the resulting secondary legislation should be subject to robust parliamentary scrutiny in order to avoid the phenomenon of "function creep", where the scope of the bill is gradually expanded beyond what Parliament originally envisaged. Terri Dowty illustrated this point:

> "The classic example was the National Pupil Database. Originally contained in the Education Act 1997 there was the provision to collect information from schools on an aggregate basis in order to plan for services. Into the School Standards and Framework Act [1998] … there was inserted an amendment, halfway through committee stage, that turned that into a power to share individual information about pupils and to specify that information in regulations." (Q 833)

359. Since then, she added:

> "We have seen a classic example of function creep, because the school census is now termly and they have gone from collecting very basic information about children to quite detailed information, including how a child gets to school in the mornings, recording behaviour and attendance data, whether they have special needs and whether they have free school meals. This is all going on to the National Pupil Database, which is, as far as we know at the moment, a permanent database without the intention to delete the content of it. That is a perfect example of a power that got through with little scrutiny because at the time there was not the same awareness of the power of databases and of information sharing." (Q 833)

360. An example is local authorities' powers under the Regulation of Investigatory Powers Act 2000 (RIPA), which we reflected on in Chapter 4. Similarly, Liberty gave the following warning in respect of the Identity Cards Act's NIR:

> "The reserved powers scattered throughout the Act allow scope for the range of uses and purposes of the NIR, and those who can have access to it, to be increased. If the NIR comes into existence then it is likely to make logistical, financial and political sense to increase the purposes it serves … 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." (p 105)

361. Dr Chris Pounder, then of Pinsent Masons, pointed out that "the NIR started life as a security system and is now a public administration, identity management and security system." (pp 281–82)

362. Some witnesses were worried that the processes for scrutinising secondary legislation were inadequate. Dr Pounder warned that "secondary legislation … is not subject to line by line scrutiny or much debate" and added that "Ministers can expect the use of their powers to be approved by Parliament

and it is a very rare occurrence that an SI [Statutory Instrument] is defeated or withdrawn; there are about 2,500 Statutory Instruments … per year and, unless the SI is technically defective, most are not challenged." (p 280) Liberty agreed that secondary legislation receives "scant Parliamentary time". (p 106)

363. Several witnesses felt that the process could be improved by the introduction of amendable secondary legislation. Gareth Crossman, the then Director of Policy at Liberty, explained that, because Parliament could not amend secondary legislation, Parliament did not have the opportunity (for example) to edit a list of bodies to whom a piece of secondary legislation would grant new surveillance powers. He asserted that "there is no constitutional reason whatsoever why Parliament could not be permitted to determine to amend resolutions" and cited the example of the Civil Contingencies Act 2004. (Q 249) Similarly, Terri Dowty suggested that "if we are going to give the Executive such far reaching powers to create legislation then perhaps there needs to be a process whereby things deemed sufficiently serious to warrant affirmative resolution actually receive proper scrutiny by committee and perhaps introduce the opportunity to amend regulations at that stage." (Q 838)

364. Whilst the concept of amending secondary legislation that enlarges surveillance and data powers may seem appealing, we do not believe that it is practical. Making secondary legislation amendable essentially turns it into primary legislation, with all the problems that this implies in terms of securing agreement between the two Houses, parliamentary time and the independence of the judiciary which rules on the legality of orders and regulations. If "function creep" is to be avoided, it will be necessary to strengthen the scrutiny of such secondary legislation in other ways.

365. One way to strengthen the scrutiny of statutory instruments in this field would be for the House of Lords Merits of Statutory Instruments Committee to flag up instruments which in its view inappropriately extend surveillance and data processing powers. Key issues for consideration would include whether the Government have shown the extension of powers to be both necessary and proportionate. **We encourage the Merits of Statutory Instruments Committee to apply the tests of necessity and proportionality to all secondary legislation which extends surveillance and data processing powers, and to alert the House in the normal way where there are any doubts about the appropriateness of the instruments.**

Enhancing the quality of scrutiny

366. We now consider more general ways of enhancing the quality of parliamentary scrutiny. One obvious measure would be to increase the involvement of the Information Commissioner in the legislative process. David Smith, Deputy Information Commissioner, told us that "where Bills are subject to parliamentary scrutiny … it is rather haphazard as to whether we get invited, whether there is investigation of our areas." He wondered whether there was "some scope to formalise that arrangement whereby we have a right to be heard or something of that sort in the process where there are significant implications in legislation for the use and collection of personal information." (Q 8) Similarly, Richard Thomas, the Information Commissioner, said that "we would like … to have a stronger right to come

forward—either the law requires some consultation with our office or that there is a duty when a new scheme is being introduced to consult with us." (Q 10) He noted that he did have a power "to make a special report to Parliament" and accepted that "it should have been used more frequently", but warned that there were resource implications. (Q 15)

367. Graham Greenleaf, Professor of Law at the University of New South Wales, went further and suggested that the Information Commissioner should be under "a statutory obligation to warn Parliament of any significant privacy dangers that he perceives in legislation or regulation." He said that the emphasis would be on the word "significant" so that the Commissioner would not have to refer minor concerns to Parliament. The advantage of a statutory duty, Professor Greenleaf explained, was that the Information Commissioner would avoid having to justify any intervention and would be less likely to face accusations of playing "partisan games". (Q 80)

368. Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), told us that the Dutch Data Protection Authority works with its national parliament and provides advice on intended legislation. (Q 513) Indeed, Professor Koops made it plain that he considered such an advisory role to be an essential part of the regulatory function:

> "I see two functions for regulatory authorities: one is to supervise the way that data protection law and also privacy law is being implemented and lived up to in practice … but I think the other role could be equally important, which is to provide parliaments with advice on intended legislation". (Q 513)

369. Dr Pounder suggested that the Information Commissioner should have the power to refer matters of concern to Parliament for consideration and action. (Q 847) This would exist in addition to the annual and extraordinary reporting processes currently set out in the Data Protection Act 1998 (DPA).

370. **We believe that the Information Commissioner should have a greater role in advising Parliament in respect of surveillance and data issues. We therefore recommend that the Government should be required, by statute, to consult the Information Commissioner on bills or statutory instruments which involve surveillance or data processing powers. The Information Commissioner could then report any matters of concern to Parliament.**

371. Several witnesses stressed the importance of Parliament, in the course of scrutiny, considering the effects on society of surveillance measures. Liberty told us that "Parliament is particularly well-placed to assess the wider societal impact of measures which interfere with personal privacy. While the courts, for example, often focus on individual cases, Parliament is better able to look at the broader picture." This was particularly important in the context of surveillance and data protection because "it is only when one aggregates the impact of such measures across the millions of people they affect that one can see the real extent of their effect on privacy and their significant constitutional implications." (p 103)

372. Professor Koops accepted the importance of such an approach, but warned that "the policy and societal debates often focus on the individual steps rather than on the entire leap, and it is questionable whether the cumulative move towards surveillance is evidence-based and well-considered." (p 173)

The reason for this, he explained, was that parliaments were "incident driven" and tended to focus on "a single measure which seems important because with this you can prevent what happened last week, and so they look at each single measure … [and] do not have the overall picture and disregard the cumulative effect which all these measures together have on privacy." (Q 507) Therefore, he suggested, "a key recommendation for legislatures is to pay more attention to empirical underpinning of surveillance measures and their cumulative effect, to commission evaluation studies, and to use sunset clauses in legislation in case a measure does not show effect." (p 173)

373. Professor Ian Loader, Director of the Centre for Criminology, University of Oxford, also identified a systemic failure to take a cumulative and evidence-based approach:

> "I sometimes think that surveillance measures in general, and let us take closed-circuit television cameras as an example, are what you might describe as destined to succeed. If it can be established that they have been a success in reducing levels of crime or fear of crime, then the answer is that we need more of them. If it can be established that they have not succeeded, then the answer is always that we need more of them … It seems to me that the consequence of that is that there is a ratcheting up process going on here. In other words, that once you put certain kinds of measures in place, it becomes very difficult to imagine the circumstances in which you could successfully take them away again, either legally, politically or culturally." (Q 610)

374. In Chapter 1, we drew attention to the spread and increase in surveillance and data collection over many years. It has been difficult for Parliament to scrutinise the piecemeal way surveillance has developed to cover so many aspects of everyday life. One way of increasing the ability of Parliament to take a more cumulative and evidence-based approach is to establish a Joint Committee of both Houses tasked specifically with considering surveillance and data issues, both through bill scrutiny and through wider policy inquiries. At the moment the remit of the JCHR only touches on surveillance and data issues insofar as they engage Convention rights. Similarly, the Constitution Committee can only consider surveillance and data powers during bill scrutiny insofar as they concern a point of principle affecting a principal part of the constitution. Furthermore both Committees already have a considerable workload. It is therefore desirable to set up a new Joint Committee that could look beyond the "individual steps" and single measures. The new Committee could scrutinise new surveillance and data processing powers against the broad policy context and consider empirical evidence on the effectiveness of the techniques involved, and on their effects on society and individual privacy. Such a Committee could build up a significant body of knowledge and employ its institutional memory to ensure continuity and consistency in legislative activity in this field.

375. We note the Canadian example of a parliamentary committee on access to information, privacy and ethics, which provides greater scrutiny of privacy protection issues. This Committee is able to subject bills to pre-legislative scrutiny.[175]

---

[175] Appendix 4, para 29.

376. **We recommend that a Joint Committee on the surveillance and data powers of the state be established, with the ability to draw upon outside research. Any legislation or proposed legislation which would expand surveillance or data processing powers should be scrutinised by this Committee.**

377. An important element in maintaining an evidence-based and cumulative view of the surveillance landscape is the evaluation of whether legislation already enacted is operating as intended. As David Feldman, Rouse Ball Professor of English Law, University of Cambridge, warned us:

> "One of the features of legislation that confers new powers on any agency is that they start by conferring it to deal with what is billed as an exceptional problem or threat, and usually the power is nicely limited and it is subject to carefully thought out safeguards which provide a graduated system for ensuring that the use of the power is properly limited and proportionate. It then becomes, as it were, normalised and increasingly drifts across into other functions, other agencies, and at the same time what tends to happen is that the safeguards, which were carefully thought out at the initial stage, get watered down, and that is a pattern which has been a common feature of police powers, data sharing powers, a whole range of powers to obtain and then use information across a very wide range of statutory fields." (Q 531)

378. The Government recently published its strategy on post-legislative scrutiny, proposing that departments should produce memoranda on most acts three years after enactment, with the relevant House of Commons select committee (or other committees where appropriate) then deciding whether to conduct further scrutiny.[176]

379. **We urge the Government to give high priority to post-legislative scrutiny of key statutes involving surveillance and data processing powers, including those passed more than three years ago. The statutes should be considered as part of a whole, rather than in isolation. This post-legislative role could be carried out effectively by a new Joint Committee on surveillance and data powers.**

---

[176] Office of the Leader of the House of Commons, *Post-legislative Scrutiny—The Government's Approach*, Cm 7320, March 2008.

CHAPTER 8: THE ROLE OF CITIZENS

Introduction

380. We have already examined the growth in surveillance and data processing in recent years. It has been said that we are in danger of sleepwalking into a surveillance society. Whilst recognising this danger, we believe that there are ways of avoiding this if action is taken now.

381. We have made recommendations relating largely to government, Parliament and the regulators. In this chapter we consider the role played by citizens in surveillance and data processing. There are two main aspects to this. The first is citizens' exercise of autonomous choices about the collection and processing of data. The second is citizens' participation in policy decisions that affect privacy and data protection. This includes practical attempts to improve transparency and public understanding, and to take account of public views and concerns in the policy making process. We also consider the state of public opinion, knowledge and beliefs about surveillance, data processing and privacy.

The individual citizen's role

382. We consider first the role of citizens in protecting the privacy of their own personal data and in controlling surveillance. The individual citizen plays an integral part within a framework of laws and other instruments for privacy protection, in terms of individual control of information, where possible, and in helping to exert collective pressure to improve practice and compliance with law.

383. The doctrine of "informational self-determination" means that the citizen controls the flow of his or her personal data. The doctrine has been judicially interpreted in Germany to give the individual the right of control, but subject to restrictions determined by the test of proportionality. Dr Lee Bygrave, Associate Professor in the Faculty of Law, University of Oslo, told us how this right has served to curb legislation involving covert online monitoring of private internet activity, thus in effect extending the right to the protection of personal computer systems. (QQ 489–91)

384. Although we recognise the difficulty in giving this principle practical effect or constitutional force in this country, in the absence of a statutory right to privacy we see it as having significant moral value in helping to restore an endangered priority in citizen-state relations. It also underpins the role of consent and individual choice in information processing.

385. The Data Protection Act 1998 (DPA) supports individual citizens' input into data protection by giving them rights to prevent processing likely to cause damage or distress or in respect of direct marketing; to oppose decisions taken on the basis of automatic data-processing; to receive compensation for damage; and to have files corrected or destroyed. The most frequently used individual right is the right to have access to one's own data. These are essential legal safeguards. But their effectiveness may be limited by the degree of effort and expense required of the citizen—the "data subject"—to exercise these rights, whether judicially or by seeking the assistance of the Information Commissioner.

Consent

386. Some legislative support to individual self-protection and "informational self-determination" is given through the principle of informed consent, which is often required in making data collection and sharing legitimate. Consent plays a part in the requirement for "fair processing" because it involves the organisation in conveying information to individuals about its processing activities. However, consent is not essential in determining whether personal data can be collected. Schedule 2 of the DPA includes consent as only one of the alternative conditions required for the processing of personal data, and Schedule 3 includes an alternative of "explicit consent" for processing "sensitive" information, including racial and ethnic origin, health, sexual life, offences, political opinions, and religious beliefs.

387. The principle of consent to data collection or to data sharing can help to give individuals some control over their data, provided it is "free, genuine and informed", as is stipulated by the *Data Sharing Review Report*, by Richard Thomas, the Information Commissioner, and Mark Walport, Director of the Wellcome Trust (the Thomas-Walport Review).[177] In common with that Review, we are sympathetic to "the instinctive view that wherever possible, people should give consent to the use or sharing of their personal information, allowing them to exercise maximum autonomy and personal responsibility",[178] although we bear in mind conceptual and practical flaws that need to be overcome.[179]

388. In practical terms, we recognise that, for many state activities and in the private sector, it is difficult to function without giving one's personal information, and that the scope for the individual to express genuine consent is narrow. The Information Commissioner, Richard Thomas, argued that, whereas supermarkets have a commercial, competitive interest in safeguarding personal data:

> "In other areas of life, when you are dealing with social services, with the police, with the tax people, with immigration you do not have the same element of choice and I think that perhaps brings us into the arena of … the constitutional issues where, at the very least, there needs to be a great deal more transparency". (Q 11)

389. Visual surveillance through CCTV and Automatic Number Plate Recognition (ANPR) systems for capturing information about moving vehicles, the National DNA Database (NDNAD)(except for volunteer samples), and other government databases including ContactPoint, are all examples where consent to data collection or "opting out" does not enter the equation. This is also true of the taxation system and many other state functions. Professor Clive Norris, Professor of Sociology and Deputy Director of the Centre for Criminological Research at the University of Sheffield, and representative of the Surveillance Studies Network, told us:

> "If we say that personal data primarily should belong to the person in whom it originated, then what is the relationship between that person and the state's holding of it and how can that person audit the information that the state holds on them? I think that this becomes

---

[177] Data Sharing Review Report, op. cit., para 5.14.

[178] ibid., para. 5.8.

[179] For example, see Manson N and O'Neill O, *Rethinking Informed Consent in Bioethics*, 2007.

> absolutely critical when that information is obtained without somebody's consent … CCTV cameras that record your number plates … [are] non-consensual. We have not consented to this act. I think as a citizen that, if the state is holding my personal information, the state should have a responsibility for demonstrating to me that it is accurate, that it is fair and that they have collected this information." (Q 67)

390. Consent is important in other areas of the public sector, but there are grey areas in which the need, let alone the possibility, of gaining consent is not clear. The Thomas-Walport Review referred to the "murky legislative framework" that leaves public service staff uncertain about, for example, whether it is permissible to share, across organisations, sensitive data about a child without consent.[180] Organisations and their agents are sometimes in doubt about when or whether consent is necessary or desirable, and about the mechanics of obtaining it. Terri Dowty, Director of Action on Rights for Children (ARCH), told us with regard to collections of children's data:

> "The Youth Justice Board says that gaining consent is a matter of good practice rather than a matter of law in order to share information about these children. The Government's guidance to the Common Assessment Framework says that a child of around 12 and perhaps even younger is competent to consent to data sharing, but the legal basis for that is unclear. The information sharing guidance that the Government issued, on the other hand, says that parents should always be involved in any decision. Unsurprisingly, practitioners are very confused, and it really is not clear what is happening." (Q 825)

391. Terri Dowty did not think that the Information Commissioner was providing sufficient or helpful advice, and thought that Parliament should look again at the question of the age of children's capacity to give consent. (QQ 826–28)

392. But the conditions for free, genuine and informed consent often fail to be met, as the Thomas-Walport Review showed.[181] This might be the case where there is a lack of transparency in the activities to which the individual is asked to consent, a false sense of choice, or an inability or unwillingness of an organisation to abide by the individual's response. There is also the question of whether fresh consent needs to be obtained where the data are to be used or disclosed for purposes other than the originally consented purpose. The extent to which consent can be subsequently revoked by the individual is a further issue.

393. Graham Greenleaf, Professor of Law at the University of New South Wales, explained some of the most important current limitations regarding consent:

> "I think that consent is an instrument of limited value in privacy statutes and it has been somewhat abused by consent not being clearly enough defined … Where genuine fully informed consent (where the individual really has the alternative to consent or not consent without being denied valuable services) is possible, of course it is one of the reasons that do justify what would otherwise be interferences with privacy. But where that fully genuine consent does not exist, it is better just to accept that the requirements should be first that there is justification for the

---

[180] Data Sharing Review Report, op. cit., para 5.27, and Box, p 38.

[181] ibid., paras 5.7–5.20.

interference and then notice that the interference is going to take place." (Q 83)

394. The feasibility of consent in the fields of public health and medical research has been a fraught issue, as the Thomas-Walport Review acknowledged.[182] There are also practical difficulties in obtaining consent, for instance from children, the elderly, and incapacitated persons. Judgments by, for example, frontline health and care workers about whether and how to obtain consent, or instead to infer it, are put to a difficult test in cases of this kind.

395. The issue of consent has also arisen in relation to the collection and retention of volunteer samples on the NDNAD. We discussed this in Chapter 4.

396. Unless the obstacles and uncertainty are overcome, we believe that the citizen will lack an important element of empowerment that could act as a safeguard. We therefore welcome the Information Commissioner's guidance on consent to data sharing, contained in his recent *Framework Code of Practice for Sharing Personal Information*,[183] which is likely to form the basis of a statutory code.

397. **We recommend that the Government, in conjunction with the Information Commissioner, undertake a review of the law governing citizens' consent to use of their personal data.**

Public opinion, beliefs and engagement

398. Public opinion is important in policy decisions within a system of representative parliamentary democracy. Public opinion is dependent on the extent of individual understanding or experience of the issues involved. Support for surveillance may be based on lack of knowledge about its methods, extent, or unintended consequences. Overcoming such lack of knowledge is difficult in the face of organisations bent on increasing their surveillance and data collection.

399. We are aware of the difficulty of conducting research into what the public feels and knows about surveillance issues. Methodological problems include focus group and sampling procedures, survey design, the phrasing of questions, and the analysis of answers. Research commissioned or conducted by government, business and the media cannot always be taken as disinterested. Assertions about what "the public" feel or want concerning surveillance are not conclusive, although they often go unchallenged. While there are few conclusive findings, we cite the results of various surveys and focus groups.

400. **We recommend that the Government bring together relevant research councils, polling organisations and government research and statistics bodies to examine ways of improving the independent gathering of public opinion on a range of issues related to surveillance and data processing.**

Public opinion and attitudes

401. Public space CCTV appears to command widespread support in the UK. The Home Secretary said in a speech on 16 December 2008:

---

[182] ibid., paras 2.31–2.32.

[183] Framework Code of Practice for Sharing Personal Information, op. cit., pp 7–8.

> "I am quite clear that we have the confidence and support of the public … on the use of CCTV cameras … CCTV has helped to reclaim our town centres for the law-abiding majority. It's playing a key role in crime prevention and in reducing the fear of crime—in turn bolstering the confidence of communities to stand up to vandalism and anti-social behaviour."[184]

402. The Minister of State at the Home Office for Crime, Policing, Counter-terrorism and Security, Vernon Coaker MP, told us:

> "I think CCTV is very popular … if I look at my own constituency where people come to see me the demand is not for less CCTV; it is always for more. Also … people see it as a very effective safety measure. I have seen all the various debates that there are about it. All I can say is that everywhere I go and for nearly everybody that I speak to CCTV has been something which promotes public safety, helps tackle crime and is fantastically reassuring." (Q 1069)

403. Councillor Hazel Harding, Leader of Lancashire County Council and Chair of the Local Government Association Safer Communities Board, agreed with this:

> "My perception and that of my colleagues from various councils is that CCTV is very popular with law-abiding members of the public who see it as a preventative and feel much safer … CCTV is something that councils are facing demands for day after day from members of the public who think it would actually make them safe and they would feel safer because of it." (Q 771)

404. The Association of Chief Police Officers (ACPO) alluded to the findings of the Leicestershire Citizens' Panel, which suggested that "the community is only too content to surrender some privacy in the interests of safety and crime reduction—and that CCTV is regarded as a highly acceptable intrusion." (p 41) On the other hand, ACPO also remarked that this popular drive for more CCTV coverage was "often against the advice and better judgement of the 'State'." (p 41)

405. We saw in Chapter 3 that the evidence of CCTV's limited and variable effectiveness tends to contradict popular beliefs. We referred to the mixed evidence about CCTV's effect on the reduction of the fear of crime, and to increases in the feeling of safety, as ascertained by attitude research.[185] Government has made considerable sums available to local authorities through bidding processes—£38.5 million for 585 schemes between 1994 and 1999, and £170 million between 1999 and 2003 for 680 schemes under the Crime Reduction Programme.[186] While the Home Office has required "genuine" public consultation to be carried out by bidders for CCTV funding,[187] there can be no certainty that the opinions elicited were informed by independent evidence of likely effectiveness and adverse consequences, given the incentive to adopt CCTV that external funding provides.

---

[184] Jacqui Smith MP, Speech to the Intellect Trade Association, *op. cit.*

[185] Gill M and Spriggs A, *Assessing the Impact of CCTV*, Home Office Research Study 292, February 2005, pp 4–5.

[186] National CCTV Strategy, op. cit., p 7.

[187] Home Office, CCTV Initiative: Application Prospectus, Section 5, para 18.

406. Some critical academic research suggests that policy "marketing" by vested interests, rather than informed and thorough local debate, results in unwarranted support for CCTV.[188] The House of Lords Science and Technology Committee's 1998 report on *Digital Images as Evidence* referred to evidence from John Burrow, the then Chief Constable of Essex:

> "He believes that when public ignorance of the capabilities and intrusions of CCTV is replaced by awareness, then it 'may well be that there will be a falling off of public confidence in the authorities having control of such systems.'"[189]

407. Looking beyond CCTV, Michael Wills MP, Minister of State in the Department of Justice with responsibility for data handling issues, told us:

> "That question of public confidence is absolutely central. If the public have no confidence in the way data is being handled they will feel much less sanguine about taking the opportunities of data sharing and society as a whole will be poorer. If they have confidence because the systems are robust and transparent—which is also crucial—then of course we can reap the benefits." (Q 992)

408. Vernon Coaker told us that the Home Office have not undertaken opinion polling in relation to public attitudes towards surveillance, "but we are going to do some polling with respect to the popularity of all this work". (Q 1034) Whilst he told us that such polling would take place "in the near future", he did not give a precise date by which it would be undertaken. (QQ 1037–39) In a subsequent letter the Minister told us that research into "public attitudes towards the type of information and data used for crime fighting and public protection purposes" would be available early in 2009. (pp 374–75) In spite of this lack of polling evidence, the Minister did feel able to assert that "I think it is the truth that people do support the use of surveillance and data collection techniques as long as they have that trust and it is proportionate and the work that is done is necessary". (Q 1034)

409. A 2003 MORI survey carried out for the Department for Constitutional Affairs found that:

> "The majority of the public (60%) say they are very or fairly concerned about how their information is handled, with 22% being **very** concerned. Only 12% are not at all concerned."[190]

410. Among those who expressed concern, many pointed in particular to a feeling of lack of control over personal information and a lack of knowledge about who would have access to what information, what is being done with it, and why it is held.[191] This picture resembles that painted by the American Civil Liberties Union in the USA: a growing number of Americans are concerned about privacy issues, although they do not always understand what happens to their data in terms of profiling and sharing.[192]

---

188 Webster C, "Closed Circuit Television and Information Age Policy Processes", in Hague B and Loader B (eds.), *Digital Democracy: Discourse and Decision Making in the Information Age*, 1999, Chapter 8, pp 116–31.

189 5th Report (1997–98): *Digital Images as Evidence* (HL 64), para 4.8, and Q 420.

190 MORI, Privacy and Data-Sharing—Survey of Public Awareness and Perceptions: Research Study Conducted for Department for Constitutional Affairs, June-July 2003, p 13.

191 ibid., p 14.

192 Appendix 4, para 57.

411. One of the most detailed surveys about surveillance issues is the 2008 pan-European Eurobarometer survey of public awareness about data protection. This suggests support in the UK for the use of surveillance practices to combat terrorism, especially in recent years. In comparison with respondents from other EU countries, proportionally more UK respondents were in favour of the unconditional monitoring of telephone calls, internet usage, credit card use, and passenger flight information, not only for suspected terrorists or with judicial supervision or equivalent safeguards. [193]

412. However, about 76 per cent of UK respondents were very or fairly concerned about how public and private organisations protect the privacy of their personal data—a figure that has remained fairly constant since 1991.[194] Amongst UK respondents, only 35 per cent thought that their personal data were properly protected, 79 per cent worried about leaving personal information on the internet, and 69 per cent did not think that our legislation could cope with the growing number of people leaving personal information on the internet.[195]

413. In a year that saw the losses of large collections of personal data by government organisations, the Information Commissioner told us:

> "Concerns are increasing. People care about the subject matter; we ask people to rank their social concerns and this year 'Protecting my personal information' has ranked second … to preventing crime; it is ahead of concerns about the environment … about unemployed … about education … [and] about health. So it has gone right up the agenda. We know now that something like nine out of ten people … have concerns about the security of their personal information … 60 per cent are saying that they feel they have lost control over the way in which their personal information is being used." (Q 33)

414. The Commissioner's research in 2007 found very high levels of public concern about organisations' use of personal information, with 94 per cent worried about both data security and the passing or selling of personal details to other organisations.[196] Only about 39 per cent thought that their personal details were sufficiently protected by existing laws and organisational practice.[197] Survey evidence cited in the Thomas-Walport Review is in general consistent with these findings.[198]

415. We were told that, in the private sector in Canada, people have generally been content to provide their personal information in order to obtain store loyalty cards and other benefits. They are concerned when particular organisations are perceived to be using data in underhand or non-transparent manners, but most Canadians do not necessarily consider the cumulative effect of handing over such data to a wide range of private organisations. There is, however, a growing awareness that data could be used in ways that result in discrimination against certain types of people.[199]

---

193 Flash Eurobarometer—The Gallup Organization, *Data Protection in the European Union: Citizens' Perceptions—Analytical Report*, Series #225, February 2008, pp 47–55.

194 ibid., pp. 7–8.

195 ibid., pp 78 (Table 4a), 82 (Table 6a); 84 (Table 7a).

196 SMSR, Report on Information Commissioner's Office, Annual Track: 2007—Individuals, September 2007, p 16.

197 ibid., p 13.

198 Data Sharing Review Report, op. cit., pp 10–11.

199 Appendix 4, para 16.

416. In the UK, focus group research conducted by the Trustguide project found that the public are tolerant of CCTV in public places but find the growth of such systems less acceptable. They are in general apprehensive about "what is perceived as increasingly heavy surveillance of day-to-day movements and activities":

> "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 … The research shows we are at a tipping point of public acceptability of surveillance and data collection." (pp 408–09)

417. Trustguide focus group members tended not to trust the Government's reported reasons for greater surveillance and data collection and "lack[ed] confidence in the state's ability to manage large scale IT projects securely and effectively." Identity cards, especially those that use biometric data, further eroded trust between the state and the citizen and were perceived as offering little personal benefit. DNA data collection was considered the most unacceptable, and "the communication of realistic restitutional measures in the event of breaches in IT systems" were perceived as better for trust than guarantees of security. People were apprehensive about "function creep"—the subsequent use of data that was collected for an explicit purpose in ways not previously stated or intended. (pp 408–11)

418. The state of public awareness, knowledge and understanding about surveillance and data collection bears upon the Information Commissioner's warning about our "sleepwalking into a surveillance society".[200] On major public sector surveillance developments, the Commissioner told us:

> "If these developments are to take place there needs to be a great deal more public debate. So many of these have happened away from any real parliamentary or public debate or scrutiny; it is only in the last year or so that we have had these questions coming up on radio shows, on television programmes, and I think now people are beginning to wake up to some of the implications." (Q 11)

419. The focus group research carried out by the Performance and Innovation Unit (later the Strategy Unit) for their 2002 report, *Privacy and Data-sharing: The Way Forward for Public Services*,[201] found that the focus groups differed in the extent to which they believed data sharing was widespread. Levels of understanding were generally modest. The research also found that "*involuntary* service users were the most likely to exaggerate its extent" whilst "*voluntary* users of public services were the most frustrated about the absence of data sharing." Some groups expressed uncertainty about which data were shared, when and with whom.[202]

420. These findings are important because, as we discussed earlier, the process of obtaining people's informed consent to collect and share data is affected by what citizens understand, or are led to understand. Public beliefs about risk are important for consent and other choices that have consequences for privacy. Dr Ian Forbes, Director of fig one Consultancy, and representative

---

[200] See para 2.

[201] Cabinet Office and Performance and Innovation Unit, *Privacy and Data-sharing: The Way Forward for Public Services,* April 2002.

[202] 6 P, Strategies for Reassurance: Public Concerns about Privacy and Data Sharing in Government—Findings from Focus Groups, Performance and Innovation Unit, 2001, pp iv–v.

of the Royal Academy of Engineering (RAE), observed that "we know that in terms of trust people mostly think in terms of risk; how risky it is if they give you this information. So they will trust you if they think the risk is appropriate. They do not know what the risks are most of the time". (Q 450)

421. Professor Angela Sasse, of University College London, and representative of the UK Computing Research Committee (UKCRC), told us:

> "Very often, where people say they do not actually care about [privacy], it is because people are not very good at assessing risks in the future, because they have not experienced the impact or nobody they know well whom they would understand and empathise with has experienced these bad effects." (Q 413)

422. Professor Martyn Thomas, independent consultant and representative of the UKCRC, illustrated this point in another context:

> "We met with a group of schoolchildren and explained to them that if they put photographs on their Facebook page and then a few days later took them down, they did not go away, and they were shocked. We have a generation of people, not just the young people but their parents as well, who simply do not understand the risk that they are running because there is not a full understanding of how the internet works". (Q 417)

423. The Eurobarometer survey revealed that a majority of UK respondents knew about specific rights and remedies available to them, but only when prompted.[203] These numbers, while consistent with the "prompted awareness" levels found in the Information Commissioner's annual tracking survey,[204] are far higher than those who can identify their rights without prompting.[205]

424. We are aware that the Information Commissioner's Office (ICO) has devoted substantial resources over recent years to promoting public knowledge and awareness of privacy intrusions and protection. However, only some 19 per cent of those surveyed professed to know about the existence of "an independent authority in the UK monitoring the application of data protection laws"—a question asked abstractly and without mentioning the ICO.[206] A survey reported in 2008 by the British Computer Society showed that 90 per cent had heard of the DPA, although their perception of what it protects them from was less accurate.[207] A similar proportion was found in the Information Commissioner's 2007 research, although this was about twice the number who were aware of the DPA in unprompted responses.[208]

425. The National DNA Database Ethics Group has recommended "better information for the public, the police, volunteers and custodial subjects on

---

[203] Data Protection in the European Union: Citizens' Perceptions—Analytical Report, op. cit., Chapter 4.

[204] Information Commissioner's Office, Annual Report 2007/08, HC 670, July 2008, p 13; Report on Information Commissioner's Office, Annual Track: 2007—Individuals, op. cit., p 15.

[205] Report on Information Commissioner's Office, Annual Track: 2007—Individuals, op. cit., p 14.

[206] Data Protection in the European Union: Citizens' Perceptions—Analytical Report, op. cit., p 104 (Table 17a).

[207] British Computer Society, *BCS Data Guardianship Survey 2008*, March 2008, p 4.

[208] Report on Information Commissioner's Office, Annual Track: 2007—Individuals, op. cit., p 17.

the use and limitations of forensic DNA analysis."[209] It sees this, in part, as important for informed consent when volunteer samples are taken.[210]

426. The Ethics Group has also considered broader ways of informing the public about the NDNAD[211] and has established a means for gathering the views of a range of stakeholder organisations on the taking and retention of DNA samples which includes human rights organisations, political parties, learned societies, statutory bodies and a Home Office unit.[212] The Ethics Group has also taken the view that public debate must take place before any decisions are taken to convert the NDNAD into a repository of the entire country's DNA characteristics.[213]

427. **We recommend that the Government and local authorities should help citizens to understand the privacy and other implications for themselves and for society that may result from the use of surveillance and data processing. Government should involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing.**

428. In the case of the NDNAD, we note that the Ethics Group has collaborated with the Human Genetics Commission's (HGC) "Citizens' Inquiry" that collected public views on the forensic use of DNA.[214]

429. Panellists drawn from the general public produced 29 core recommendations which the HGC is subsequently considering. These include a nationwide public awareness campaign, and more substantive proposals concerning DNA retention, rules about the collection of samples, the governance of the NDNAD, and other issues.[215]

430. We are impressed by the use of this technique for eliciting informed opinions by citizens and thus helping to shape policies.

431. Professor Sasse told us:

> "In my view Government has recently been very fond of just holding consultations which are effectively rubber-stamping, opinion-poll-type things. I do not have a great deal of faith in those. If you contrast them then with more detailed investigations where people actually have a chance to discuss scenarios that personally concern them and then to relate their decisions, what is reported is quite different. It needs to be a more in-depth engagement." (Q 458)

432. **We recommend that the Government should undertake an analysis of public consultations and their effectiveness, and should explore opportunities for applying versions of the Citizens' Inquiry technique to surveillance and data processing initiatives involving databases.**

---

209 1st Annual Report of the Ethics Group: National DNA Database, op. cit., Recommendation E, p 21.

210 ibid., para 5.19.

211 ibid., pp 54–56.

212 ibid., pp 47–49.

213 ibid., p 26.

214 ibid., p. 50.

215 *A Citizens' Inquiry into the Forensic Use of DNA and the National DNA Database: Citizens' Report,* July 2008.

Transparency and public engagement

433. The openness of organisations, both about their personal information and surveillance plans and practices, and about ways in which the public can be more effectively involved in understanding and shaping them, is important.

434. If trust in relationships between citizens and the state is to be maintained, public understanding of surveillance and the way in which personal data are processed must involve organisational transparency, starting at an early stage in the Government's policy proposals. The Thomas-Walport Review emphasised transparency and drew a connection with public trust. It recommended six "good-practice steps" for organisations to take to increase transparency, most involving clearer and better information for the public about data sharing practices.[216] The Government have restated their commitment "to ensuring information sharing is undertaken in a transparent and controlled manner".[217]

435. The House of Commons Home Affairs Committee's report, *A Surveillance Society?*, recommended that "the Home Office should work with the Information Commissioner to raise public awareness of how the Home Office collects, stores, shares and uses personal information."[218] The Information Commissioner has expressed his disappointment that the Government's response does not make any specific commitment to this.[219]

436. **We share the Information Commissioner's disappointment that the Government have not made a specific commitment to working with the Information Commissioner's Office to raise public awareness. We recommend that the Government reconsider this matter and commit to a plan of action agreed with the Information Commissioner.**

437. The Government have also drawn attention to the Home Office's Information Charter,[220] which is "aimed at raising public awareness".[221] The Government now promote the publication of Information Charters, enjoining them on all departments as a means of transparency.[222] There are existing examples of privacy statements on departmental websites.[223] The Government's response to the Coleman Report, *Protecting Government Information*, also cited the Charter as a transparency tool.[224]

438. The model Charter's six undertakings do not explain key terms and issues concerning data retention periods, the rules for sharing, and the necessity for collection. The citizen is required to contact the department for further

---

216 Data Sharing Review Report, op. cit., para 8.14.

217 Government Response to Data Protection and Human Rights, op. cit., Appendix (p 11).

218 *A Surveillance Society?*, op. cit., para 162.

219 Information Commissioner's Office, Information Commissioner's Formal Response to the House of Commons Home Affairs Committee Report 'A Surveillance Society?', para 5.3.

220 See http://www.homeoffice.gov.uk/documents/information-charter?view=Binary.

221 The Government Reply to A Surveillance Society?, op. cit., p 9.

222 Data Handling Procedures in Government: Final Report, op. cit., p 23, paras 2.43, 3.8, and Annex IV.

223 ibid., Annex IV. For example see Department for Children, Schools and Families, http://www.dcsf.gov.uk/copyright/pdf/psg-english1.pdf; HM Revenue & Customs, http://www.hmrc.gov.uk/about/privacy.htm; and Department for Transport, http://www.dft.gov.uk/about/informationcharter/

224 Data Handling Procedures in Government: Final Report, op. cit., p 39. See Protecting Government Information—Independent Review of Government Information Assurance, op. cit.

details. The Charter appears to derive from the Performance and Innovation Unit's document that was put out for public consultation in 2002.[225]

439. In the interests of greater transparency, we support the Government's decision to require departments to promulgate an Information Charter. However, we remain to be convinced that the latest initiative will materially improve government transparency and public understanding.

440. **We recommend that the Government improve the design of the Information Charter, and report regularly to Parliament on the measures taken to publicise the Charter and on their monitoring of the public response to it.**

441. The Council for Science and Technology (CST) have also argued strongly for the promotion of better public understanding of information processes, including data sharing, and deeper public engagement with government. Their 2005 report, *Better Use of Personal Information: Opportunities and Risks*, recommended "dialogue with the public and stakeholders on the full range of benefits and risks, in particular to individual citizens as well as to society and to government".[226]

442. The CST have outlined desirable procedures, and commissioned focus group discussions that explored public perceptions of the current and future use of personal data by public bodies, as well as public attitudes. Other than on information practices in the health sector, these discussions revealed considerable scepticism and lack of trust, a view that privacy protection was paramount, a demand for greater clarity in the reasons for sharing information, and feelings of powerlessness in the face of the state's use of personal information.[227]

443. The CST have identified deficiencies in the way government engages with the general public's concerns over policy developments involving the use of science and technology. They have pressed government to adopt certain proposals which include the early identification of emerging issues, ministerial engagement with and commitment to public dialogue, governance arrangements for dialogue, allocation of resources, and evaluation and learning.[228] We believe that the proposals are adaptable for use in surveillance and data collection policies.

444. The Government's response stated that they agreed "that public dialogue on science and technology must be driven forward within an explicit framework with top-level commitment." The Government thought that the CST's overarching framework was "sensible", and reflected the requirements of Cabinet Office guidance on consultation. It was conceded that "more work is needed to embed the principles across government … and we will continue to review and revise the guiding principles … and are taking steps to open up the process of developing policy to a wider range of voices." The

---

225 Performance and Innovation Unit, Privacy and Data-sharing: The Way Forward for Public Services, op. cit., p 58.

226 Better Use of Personal Information: Opportunities and Risks, op. cit., p 2.

227 OPM, Research into the Use of Personal Datasets held by Public Sector Bodies—Final Report for Council for Science and Technology (draft), October 2005, pp 2–3.

228 Council for Science and Technology, Policy Through Dialogue: Informing Policies Based on Science and Technology, March 2005.

Government also agreed that "public dialogue should be undertaken within a clear governance structure", but that "a flexible approach is necessary."[229]

445. **We support the Government's acceptance of the Council for Science and Technology's recommendations for public dialogue and engagement in terms that commit them to the further development of techniques, governance structures, and relationships both within government and with external bodies. We recommend that the Government report to Parliament on the formal requirements which they are placing on departments and agencies to ensure that this commitment extends to policies and practices involving surveillance and data processing.**

Collective efforts

446. We now consider collective efforts on behalf of the public to limit intrusive surveillance and data processing. Non-governmental organisations (NGOs) are among those who sustain these efforts.[230] Our visit to Canada and the USA left us with the impression that many civil liberties and campaign groups in those countries play a particularly prominent and well-respected role in relation to these issues.

447. Dr Bygrave said that they are "important in igniting public debate." (Q 508) Large scale pressure group campaigns involving public protest have had occasional success, for example in influencing the Australian government to abandon its plans for a national identity card in 1986,[231] and in influencing the French government to modify substantially its EDVIGE proposal for a very large and intrusive database in 2008.[232]

448. In this country, many groups, including Liberty, JUSTICE, Privacy International and the Foundation for Information Privacy Research (FIPR) operate across a broad front of issues. Some, such as NO2ID, campaign on single issues such as identity cards, whilst others, including the Enterprise Privacy Group and the British Computer Society, aim at raising the level of awareness and good practice among groups such as industry and business.

449. Some NGOs assist the parliamentary scrutiny of legislation and the work of the ICO. FIPR claims success in improving a number of pieces of surveillance and data processing legislation, including the Regulation of Investigatory Powers Act 2000 (RIPA), the Health and Social Care Act 2001, the Anti-Terrorism, Crime and Security Act 2001, and in contributing to policy criticism on children's databases.[233] Liberty was prominent in briefing on the Identity Cards Act. Activities of this kind are of particular importance in the area of surveillance and information systems, where Parliament may particularly value the technical knowledge necessary for effective scrutiny to take place.

---

[229] Council for Science and Technology Report, Policy through Dialogue, Published March 2005—Government Response, September 2005. See especially paras 4–7, 10.

[230] Bennett C, The Privacy Advocates: Resisting the Spread of Surveillance, 2008.

[231] Davies S, Big Brother: Britain's Web of Surveillance and the New Technological Order, 1996, Chapter 7.

[232] "French File EDVIGE Revised After Huge Civil Society Mobilization", *EDRI-gram Number 6.18*, 24 September 2008.

[233] See http://www.fipr.org/achievements.html

450. Professor Bert-Jaap Koops, Professor of Law and Technology at Tilburg University Institute for Law, Technology and Society (TILT), told us:

> "Pressure groups are very important because they can play a role in debates by giving information, by highlighting possible effects that in the general debates tend to be overlooked, but … they are usually quite small, with a few people, often volunteers, with limited resources, and so there are only a limited amount of topics that they can monitor. More importantly, if the question is: do they not fill up the democratic deficit to a large extent? No, they never can, because they have no power. Their function is to highlight evidence, to signal, to give information, but they have no influence directly … they have no power to say this measure should be not adopted, like parliaments, like the courts and data protection commissioners have, so they could never fill up the democratic deficit." (Q 511)

451. **We believe that the Government should involve non-governmental organisations in the development and implementation of surveillance and data processing policies with significant implications for the citizen.**

CHAPTER 9: RECOMMENDATIONS

452. We regard privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers as necessary conditions for the exercise of individual freedom and liberty. Privacy and executive and legislative restraint should be taken into account at all times by the executive, government agencies, and public bodies. (paragraph 144)

Recommendations relating to the commissioners

453. Before introducing any new surveillance measure, the Government should endeavour to establish its likely effect on public trust and the consequences for public compliance. This task could be undertaken by an independent review body or non-governmental organisation, possibly in conjunction with the Information Commissioner's Office. (paragraph 110)

454. The Government should consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government and private surveillance practices on the rights of the public at large under Article 8 of the European Convention on Human Rights. (paragraph 137)

455. We regret that the Government have often failed to consult the Information Commissioner at an early stage of policy development with privacy implications. We recommend that the Government instruct departments to consult the Information Commissioner at the earliest stages of policy development and that the Government should set out in the explanatory notes to bills how and when they consulted the Information Commissioner, and with what result. (paragraph 231)

456. We welcome the Government's decision to provide a statutory basis for the Information Commissioner to carry out inspections without consent of public sector organisations which process personal information systems, but regret the decision not to legislate for a comparable power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide. In addition, the protection of citizens' data may in the absence of legislation be vitiated given the growing exchange of personal data between the public and private sectors. (paragraph 238)

457. We welcome the new powers for the Information Commissioner to levy fines on data controllers for deliberately or recklessly breaching the data protection principles, and we recommend that the Government bring these powers into force as soon as possible. The maximum level of penalties should mirror that available to comparable regulators, and should not be disproportionate. This must be subject to an appropriate appeals procedure. (paragraph 243)

458. We recommend that the Chief Surveillance Commissioner and the Interception of Communications Commissioner should introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner. (paragraph 257)

459. We recommend that the Investigatory Powers Tribunal publicise its role, and make its existence and powers more widely known to the general public. (paragraph 259)

460. We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs. We also recommend that the Government—after public consultation—consider introducing a similar system for the private sector. (paragraph 307)

461. We believe that the Information Commissioner should have a greater role in advising Parliament in respect of surveillance and data issues. We therefore recommend that the Government should be required, by statute, to consult the Information Commissioner on bills or statutory instruments which involve surveillance or data processing powers. The Information Commissioner could then report any matters of concern to Parliament. (paragraph 370)

462. We recommend that the Government, in conjunction with the Information Commissioner, undertake a review of the law governing citizens' consent to use of their personal data. (paragraph 397)

463. We share the Information Commissioner's disappointment that the Government have not made a specific commitment to working with the Information Commissioner's Office to raise public awareness. We recommend that the Government reconsider this matter and commit to a plan of action agreed with the Information Commissioner. (paragraph 436)

Recommendations relating to the National DNA Database

464. We believe that DNA profiles should only be retained on the National DNA Database (NDNAD) where it can be shown that such retention is justified or deserved. We expect the Government to comply fully, and as soon as possible, with the judgment of the European Court of Human Rights in the case of *S. and Marper v. the United Kingdom*, and to ensure that the DNA profiles of people arrested for, or charged with, a recordable offence but not subsequently convicted are not retained on the NDNAD for an unlimited period of time. (paragraph 197)

465. Whilst a universal National DNA Database would be more logical than the current arrangements, we think that it would be undesirable both in principle on the grounds of civil liberties, and in practice on the grounds of cost. (paragraph 200)

466. We recommend that the law enforcement authorities should improve the transparency of consent procedures and forms in respect of the National DNA Database (NDNAD). We believe that the DNA profiles of volunteers should as a matter of law be removed from the NDNAD at the close of an inquiry unless the volunteer consents to its retention. (paragraph 208)

467. We are concerned that the National DNA Database (NDNAD) is not governed by a single statute. We recommend that the Government introduce a bill to replace the existing regulatory framework, providing an opportunity to

reassess the rules on the length of time for which DNA profiles are retained, and to provide regulatory oversight of the NDNAD. (paragraph 212)

Recommendations relating to CCTV

468. We recommend that the Home Office commission an independent appraisal of the existing research evidence on the effectiveness of CCTV in preventing, detecting and investigating crime. (paragraph 82)

469. We recommend that the Government should propose a statutory regime for the use of CCTV by both the public and private sectors, introduce codes of practice that are legally binding on all CCTV schemes and establish a system of complaints and remedies. This system should be overseen by the Office of Surveillance Commissioners in conjunction with the Information Commissioner's Office. (paragraph 219)

Recommendations for legislation and the legislative process

470. We welcome the UK Computing Research Committee's suggestion that the encryption of personal data should be mandatory in some circumstances. Organisations should avoid connecting to the internet computers which contain large amounts of personal information. We recommend that the Government introduce appropriate regulations. (paragraph 117)

471. We recommend that the Government undertake a review of the administrative procedures set out in the Regulation of Investigatory Powers Act 2000 so as to resolve the contrasting views expressed by the Association of Chief Police Officers (ACPO) and the Office of Surveillance Commissioners about the effectiveness of the current legal framework and the system of authorisations. (paragraph 159)

472. We recommend that the Government consultation on proposed changes to the Regulation of Investigatory Powers Act 2000 should consider whether local authorities, rather than the police, are the appropriate bodies to exercise such powers. If it is concluded that they are the appropriate bodies, we believe that such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years. We recommend that the Government take steps to ensure that these powers are only exercised where strictly necessary, and in an appropriate and proportionate manner. (paragraph 177)

473. We are concerned that three different offices overseeing the operation of the Regulation of Investigatory Powers Act 2000 (RIPA) may result in inefficiencies and disjointed inspection. We recommend that the Government examine the feasibility of rationalising the inspection system and the activities of the three RIPA Commissioners. (paragraph 252)

474. We are concerned that primary legislation in the fields of surveillance and data processing all too often does not contain sufficient detail and specificity to allow Parliament to scrutinise the proposed measures effectively. We support the conclusion of the Joint Committee on Human Rights that the Government's powers should be set out in primary legislation, and we urge the Government to ensure that this happens in future. We will keep this matter under close review in the course of our bill scrutiny activities. (paragraph 357)

475. We urge the Government to give high priority to post-legislative scrutiny of key statutes involving surveillance and data processing powers, including those passed more than three years ago. The statutes should be considered as part of a whole, rather than in isolation. This post-legislative role could be carried out effectively by a new Joint Committee on surveillance and data powers. (paragraph 379)

Other specific actions for the Government

476. We recommend that the Government should instruct government agencies and private organisations involved in surveillance and data use on how the rights contained in Article 8 of the European Convention on Human Rights are to be implemented. The Government should provide clear and publicly available guidance as to the legal meanings of necessity and proportionality. We recommend that a complaints procedure be established by the Government and that, where appropriate, legal aid should be made available for Article 8 claims. (paragraph 134)

477. We recommend that the Government consider introducing a system of judicial oversight for surveillance carried out by public authorities, and that individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result. We recommend that compensation should be available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers conferred by the Regulation of Investigatory Powers Act 2000. (paragraph 163)

478. We recommend that the Government's development of identification systems should give priority to citizen-oriented considerations. (paragraph 268)

479. We agree with the recommendation of the Joint Committee on Human Rights that the role of data protection minister should be enhanced and its profile elevated, and are disappointed that the Government's response has not grasped the main point about the need for more effective central leadership. The Government should report to the House through this Committee on the feasibility of having Ministry of Justice (MoJ) lawyers working in other departments and reporting to the MoJ on departmental policies with data protection implications, and of certification of legislative compatibility with the Human Rights Act 1998. This should be in conjunction with the current system of certification of compatibility by the Minister in charge of each bill going through Parliament. (paragraph 290)

480. We support the recommendations made in the Thomas-Walport *Data Sharing Review Report* for changes in organisational cultures, leadership, accountability, transparency, training and awareness, and welcome the Government's acceptance of them. We urge the Government to report on their progress to Parliament. (paragraph 292)

481. We recommend that the Government devote more resources to the training of individuals exercising statutory surveillance powers under the Regulation of Investigatory Powers Act 2000, with a view to improving the standard of practice and respect for privacy. We recommend that the principles of necessity and proportionality are publicly described and that the application of these principles to surveillance should be consistent across government. (paragraph 323)

482. We believe that encryption has a vital role to play in ensuring the security of data, and that the Government should insist upon its use as appropriate throughout the public and private sectors. (paragraph 331)

483. In the interests of strengthening the protection of personal data, we urge the Government to make the Manual of Protective Security subject to regular and rigorous peer review. (paragraph 342)

484. In the light of the potential threat to public confidence and individual privacy, we recommend that the Government should improve the safeguards and restrictions placed on surveillance and data handling. (paragraph 345)

485. We recommend that the Government review their procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems. (paragraph 349)

486. We recommend that the Government bring together relevant research councils, polling organisations and government research and statistics bodies to examine ways of improving the independent gathering of public opinion on a range of issues related to surveillance and data processing. (paragraph 400)

487. We recommend that the Government and local authorities should help citizens to understand the privacy and other implications for themselves and for society that may result from the use of surveillance and data processing. Government should involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing. (paragraph 427)

488. We recommend that the Government should undertake an analysis of public consultations and their effectiveness, and should explore opportunities for applying versions of the Citizens' Inquiry technique to surveillance and data processing initiatives involving databases. (paragraph 432)

489. We recommend that the Government improve the design of the Information Charter, and report regularly to Parliament on the measures taken to publicise the Charter and on their monitoring of the public response to it. (paragraph 440)

490. We support the Government's acceptance of the Council for Science and Technology's recommendations for public dialogue and engagement in terms that commit them to the further development of techniques, governance structures, and relationships both within government and with external bodies. We recommend that the Government report to Parliament on the formal requirements which they are placing on departments and agencies to ensure that this commitment extends to policies and practices involving surveillance and data processing. (paragraph 445)

491. We believe that the Government should involve non-governmental organisations in the development and implementation of surveillance and data processing policies with significant implications for the citizen. (paragraph 451)

Recommendations relating to Parliament

492. We welcome the Government's plans for better data handling. We recommend that the Government's report on progress on data handling and security be scrutinised by parliamentary committees. (paragraph 337)

493. We encourage the Merits of Statutory Instruments Committee to apply the tests of necessity and proportionality to all secondary legislation which extends surveillance and data processing powers, and to alert the House in the normal way where there are any doubts about the appropriateness of the instruments. (paragraph 365)

494. We recommend that a Joint Committee on the surveillance and data powers of the state be established, with the ability to draw upon outside research. Any legislation or proposed legislation which would expand surveillance or data processing powers should be scrutinised by this Committee. (paragraph 376)

Recommendation relating to all public and private sector organisations

495. As surveillance is potentially a threat to privacy, we recommend that before public or private sector organisations adopt any new surveillance or personal data processing system, they should first consider the likely effect on individual privacy. (paragraph 103)

APPENDIX 1: SELECT COMMITTEE ON THE CONSTITUTION

The members of the Committee which conducted this inquiry were:

Viscount Bledisloe (until 26 November 2008)
Lord Goodlad (Chairman)
Lord Lyell of Markyate
Lord Morris of Aberavon
Lord Norton of Louth
Baroness O'Cathain (until 26 November 2008)
Lord Pannick
Lord Peston
Baroness Quin
Lord Rodgers of Quarry Bank
Lord Rowlands
Lord Shaw of Northstead
Lord Smith of Clifton (until 26 November 2008)
Lord Wallace of Tankerness
Lord Woolf

Declaration of Interests

BLEDISLOE, Viscount

**12(g) Controlling shareholdings*
Shareholding in Peter Cheyney Ltd (a private company) (with family)
**13(a) Significant shareholdings*
Shareholding in Peter Cheyney Ltd (a private company)
**13(b) Landholdings*
Together with family trusts, ownership and management of a landed estate in West Gloucestershire, engaged in farming, forestry, property etc

GOODLAD, Lord

**12(f) Regular remunerated employment*
Member, International Advisory Council GFTA Analytics Ltd
15(d) Office-holder in voluntary organisations
Sir Robert Menzies Memorial Trust
Opera Australia Capital Fund

LYELL OF MARKYATE, Lord

**13(b) Landholdings*
Shared ownership with my wife of a house in London, a property in Burgundy and some farmland, woodlands, and a pair of cottages in Hertfordshire
15(a) Membership of public bodies
Chairman of the St Albans Cathedral Trust (until October 2007)
Member of the Court of the Universities of Hertfordshire and Luton
15(b) Trusteeships of cultural bodies
Chairman of the Federation of British Artists (the Mall Galleries) (a charity)
(I took up office at the meeting of the board on 19 July 2007)

MORRIS OF ABERAVON, Lord

15(a) Membership of public bodies
Chancellor of University of Glamorgan
Hon Fellow of Gonville of Caius College, Cambridge
Hon Fellow of University College of Wales, Aberystwyth
Hon Fellow of University College of Wales, Swansea

Hon Fellow of Trinity College Carmarthen
Bencher of Gray's Inn
Member of Council of Prince of Wales' Trust (Cymru)
Prime Minister's Advisory Committee on Business Appointments

NORTON OF LOUTH, Lord

**12(f) Regular remunerated employment*
Professor of Government, University of Hull (Director, Centre for Legislative Studies)
Director of Studies, Hansard Society
15(a) Membership of public bodies
Governor, King Edward VI Grammar School, Louth
15(b) Trusteeships of cultural bodies
Trustee, History of Parliament Trust
Trustee, Elizabeth Russell Fund (a charity)
15(c) Office-holder in pressure groups or trade unions
Chairman, Conservative Academic Group
Member, Advisory Board, Centre for Policy Studies
Member, Committee, Conservative History Group
15(d) Office-holder in voluntary organisations
Vice President, Political Studies Association of the UK
Member of Council, Hansard Society for Parliamentary Government
Editor, Journal of Legislative Studies (unremunerated but published by commercial publisher)
Council Member, Constitution Unit
16(b) Voluntary organisations
Member, Study of Parliament Group

O'CATHAIN, Baroness

**12(e) Remunerated directorships*
Director, South East Water plc (until 31 March 2008)
**12(i) Visits*
Visit to Azerbaijan in December 2006 as guest of the Government of Azerbaijan
Visit to Azerbaijan in June 2008 as guest of the Parliament of Azerbaijan
Attendance at annual conference in Kuwait (15–20 November 2008) organised by GOPAC (Global Organization of Parliamentarians Against Corruption) on Political Ethics and Conflict of Interest for Parliamentarians; travel expenses paid by House of Lords but accommodation etc paid by ARPAC (Arab Region Parliamentarians Against Corruption) in collaboration with GOPAC and the Westminster Foundation for Democracy and others (27 December 2008)
15(b) Trusteeships of cultural bodies
Chairman of Appeal Board and Trustee, Brooklands Museum

PANNICK, Lord

**12(f) Regular remunerated employment*
Practising member of the Bar
Fortnightly column on legal issues for The Times
15(a) Membership of public bodies
Fellow of All Souls College, Oxford
Hon. Fellow of Hertford College, Oxford
15(d) Office-holder in voluntary organisations
Chairman of the Legal Friends of The Hebrew University, Jerusalem
Bencher of Gray's Inn

PESTON, Lord

**12(e) Remunerated directorships*
Chairman of the Pharmaceutical Price Regulation Scheme Arbitration Panel
15(d) Office-holder in voluntary organisations
Vice President, Speakability

QUIN, Baroness

15(a) Membership of public bodies
Member of Academic Board of Wilton Park
Member of Durham Cathedral Council ***(unpaid)***
15(d) Office-holder in voluntary organisations
President, Gateshead Arthritis Care Association
16(b) Voluntary organisations
Chair of Franco-British Council

RODGERS OF QUARRY BANK, Lord

No relevant interests

ROWLANDS, Lord

**12(d) Non-parliamentary consultant*
Consultant to the National Training Federation, Wales
Consultant to Tydfil Training, Merthyr Tydfil
**12(e) Remunerated directorships*
Chairman, More Than Just a Game
**13(d) Hospitality or gifts*
I have occasionally been a guest of Dyfed Steels at the Llanelli/Scarlets' matches
15(b) Trusteeships of cultural bodies
Trustee and Member of the History of Parliament Trust
15(d) Office-holder in voluntary organisations
Trustee of the Winston Churchill Memorial Fund for travelling scholarships
16(b) Voluntary organisations
Member of the Pfizer Foundation on health inequalities

SHAW OF NORTHSTEAD, Lord

No relevant interests

SMITH OF CLIFTON, Lord

15(d) Office-holder in voluntary organisations
Member, Democratic Audit Advisory Committee
Vice Patron, Artificial Heart Fund
Vice Patron, Appeal Fund, London School of Osteopathy
Director, Government & Opposition Ltd
Director/Trustee, Democratic Audit Ltd

WALLACE OF TANKERNESS, Lord

**12(d) Non-parliamentary consultant*
Ad hoc consultancy arrangement with Aquatera Ltd, a provider of environmental and sustainability services, with particular interests in the renewable energy sector
Consultancy on Scottish Parliament and Scottish parliamentary matters, with Simpson & Marwick WS, Edinburgh. This consultancy involves advising on issues and procedures in relation to the Scottish Parliament
Consultancy with Quatro Public Relations in relation to specific renewable energy projects
Work in relation to renewable energy policy and developments is also undertaken for one particular company that is a client of Quatro and working with this client involves the member in arranging meetings with public bodies

in Scotland, writing briefings and reports and possibly attending meetings between members of the Scottish Executive and the client company
**12(e) Remunerated directorships*
Director and Chairman, Northwind Associates Ltd (wind energy)
Director and Chairman, Jim Wallace Consultancy Ltd (general public affairs, speech making, articles)
**12(f) Regular remunerated employment*
Employed by Jim Wallace Consultancy Ltd
**12(g) Controlling shareholdings*
80% shareholding in Jim Wallace Consultancy Ltd – general consultancy on public policy issues, speech making, articles
**13(a) Significant shareholdings*
20% interest in Northwind Associates Ltd (wind energy)
**13(b) Landholdings*
One-half share in two dwelling houses in Annan, Dumfresshire (no rental income)
One-half share in 2 acre field at Annan, Dumfresshire
15(a) Membership of public bodies
Non-practicing member of Faculty of Advocates
Hon. Professor in Institute of Petroleum Engineering, Heriot Watt University
Member of the Commission on Scottish Devolution
15(d) Office-holder in voluntary organisations
Board Member, St. Magnus Festival Ltd (unremunerated)
Chair of Relationships Scotland (the new organisation which embodies the merger between Family Mediation Scotland and Relate Scotland) (from 1 April 2008) ***(unpaid)***
Board Member, Centre for Scottish Public Policy (independent think tank) ***(unpaid)***
Consultancy with Hays Special Recruitment

WOOLF, Lord

**12(f) Regular remunerated employment*
Non-permanent judge of Hong Kong Final Court of Appeal – Law Lord
Advisor to CEDR on mediation issues
Chairman of the Bank of England's Financial Markets Law Reform Committee
June 2007-May 2008: Chairman, of the Woolf Committee, which reviewed and propose standards of ethics and integrity for adoption in existing and future contracts for the manufacture and supply of arms by BAE Systems Limited
Senior Judge, Commercial Court, Qatar
Chancellor of the Open University of Israel
Regular income from speeches, writing articles and books on the above subjects
15(d) Office-holder in voluntary organisations
President, Chairman or Patron of numerous voluntary bodies working in the areas of prison and justice

APPENDIX 2: LIST OF WITNESSES

The following witnesses gave evidence. Those marked with * gave oral evidence.

Mr Andrew A Adams

AD Group

* Association of Chief Police Officers (ACPO)

Mr Martin Beaumont

Trevor Bedeman

* Mr Mike Bradford, Director or Regulatory and Consumer Affairs, Experian

* British Computer Society

* Dr Lee Bygrave, Associate Professor, Faculty of Law, University of Oslo

The e-Assessment in Child Welfare Research Project

* Vernon Coaker MP

The Customer's Voice

Mr Charles Farrier

* Professor Jörg Fedtke, Faculty of Laws, UCL

* Professor David Feldman, Rouse Ball Professor of English Law, University of Cambridge

Finance & Leasing Association (FLA)

Foundation for Information Policy Research (FIPR)

* GeneWatch UK

Tarique Ghaffur

* Professor Graham Greenleaf, Professor of Law, University of New South Wales, Australia

* Mr Tim Hayward, Acting Director of the intercept modernisation programme Home Office

* Dr Gus Hosein, London School of Economics and Political Science

* Mr Peter Hustinx

* Professor Peter Hutton, Chairman, National DNA Database Ethics Group

* Information Commissioner's Office (ICO)

Joint Council for the Welfare of Immigrants

* JUSTICE

* Sir Paul Kennedy, Interception of Communications Commissioner

* Professor Bert-Jaap Koops, Tilburg University Institute for Law Technology and Society (TILT), the Netherlands

Dr Hazel Lachohee and Dr Andy Phippen

* Professor Graeme Laurie, University of Edinburgh

The Law Society of Scotland

* Liberty
* Professor Ian Loader
* Local Government Association (LGA)

LSE Identity Project

* Mr Tony McNulty, MP
* Professor Janice Morphet

Mr David Moss

* National Policing Improvement Agency (NPIA)

Network Research Group

Dr Daniel Neyland

NO2ID

NO2ID Hackney & Shoreditch

* Professor Dawn Oliver, Professor of Constitutional Law, UCL

The Open Rights Group

* Dr Chris Pounder, Pinsent Masons
* Sir Christopher Rose, Chief Surveillance Commissioner, Office of Surveillance Commissioners
* Royal Academy of Engineering

Runnymede Borough Council

* Mr Toby Stevens, Director, Enterprise Privacy Group
* Surveillance Studies Network
* Martyn Thomas, independent consultant and UK Computing Research Committee

Dr T Thomas

Hugh Tomlinson QC

* UK Computer Researching Committee (UKCRC)
* Mr Philip Virgo, Secretary General, EURIM

G M Walkley

* Mr Stephen Webb, Acting Director of policing policy and operations, Home Office
* Dr Victoria Williams
* Mr Michael Wills, MP and Ms Belinda Crowe

APPENDIX 3: ACRONYMS

ACLU	American Civil Liberties Union
ACPO	Association of Chief Police Officers
AmI	Ambient intelligence
ANPR	Automatic Number Plate Recognition
ARCH	Action Rights for Children
BERR	The Department for Business, Enterprise and Regulatory Reform
CCTV	Closed Circuit Television
CHIS	Covert human intelligence sources
CIFAS	Credit Industry Fraud Avoidance System
CLG	Department of Communities and Local Government
CRM	Customer-relationship marketing
CST	Council for Science and Technology
DHS	US Department of Homeland Security
DoJ	Canadian Department of Justice
DVA	Driver and Vehicle Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EURIM	European Information Society Group
DCSF	The Department for Children, Schools and Families
DHS	The US Department of Homeland Security
DNA	Deoxyribonucleic acid
DPA	Data Protection Act 1998
DWP	The Department for Work and Pensions
FIPR	Foundation for Information Policy Research
FOIA	Freedom of Information Act 2000
HGC	Human Genetics Commission
HMRC	Her Majesty's Revenue and Customs
HRA	Human Rights Act 1998
ICT	Information and Communication Technology
ICO	Information Commissioner's Office
IPT	Investigatory Powers Tribunal
JCHR	The Joint Committee on Human Rights
LACORS	Local Authority Coordinators of Regulatory Services
LGA	Local Government Association
LSE	London School of Economics

MOD	Ministry of Defence
MoJ	Ministry of Justice
NDNAD	The National DNA Database
NGO	Non-governmental organisation
NHS CRS	The National Health Service Care Records Service
NIR	The National Identity Register
NPIA	National Policing Improvement Agency
OSC	Office of Surveillance Commissioners
PETs	Privacy-enhancing technologies
PIA	Privacy Impact Assessment
RAE	Royal Academy of Engineering
RFID	Radio Frequency Identification
RIPA	Regulation of Investigatory Powers Act 2000
TFL	Transport for London
TILT	The Tilbury University Institute for Law, Technology and Society
UKCRC	UK Computing Research Committee

APPENDIX 4: VISIT NOTE—21–25 APRIL 2008

1. This note constitutes the official record of the Committee's visit to Canada and the United States of America as part of the inquiry into surveillance and data collection.

CANADA

Department of Justice Canada and the Public Prosecution Service of Canada

2. The participants from the Department of Justice were Mr Stanley Cohen (Senior General Counsel, Human Rights Law Section); and Ms Sarah Geh and Mr Shawn Scromeda (Counsels, Human Rights Law Section). Mr George Dolhai (Acting Deputy Director of Public Prosecutions, Criminal Litigation and Organized Crime Branch) participated from the Public Prosecution Service of Canada.

3. The Canadian Charter of Rights and Freedoms—a bill of rights entrenched in the Canadian Constitution passed in 1982—supplemented the earlier Bill of Rights which had on occasion been described as 'toothless'. The Charter played an important role in protecting personal privacy (particularly in terms of surveillance) but the jurisprudence was still immature. There had been an 'ebb and flow' in the decisions of the courts and it is possible that, in future, they may not be as favourable towards privacy as previously. One key provision of the Charter was section 8. Although this section did not provide an explicit right to privacy—it is worded as a protection against "unreasonable search or seizure"—the jurisprudence of the courts had gone some way towards establishing such a right under this provision, as well as under the Charter's fundamental justice provision, section 7.

4. One of the responsibilities of the Department of Justice (DoJ) was to monitor developments in this field and to examine different government departments' proposals for data sharing provisions etc. DoJ lawyers provided advisory services to all government departments. These lawyers worked in the legal services of individual departments and at Justice Headquarters, and provided advice on government initiatives that may affect privacy interests. In addition, the Minister of Justice had a statutory responsibility to certify that legislation was compatible with the Charter of Rights.

5. The privacy commissioners (one at the federal level and one in each province and territory) played an important role in monitoring information sharing across government. In general, the commissioners were concerned about the growth of information sharing and the aggregation of ever greater amounts of data. There was also significant concern expressed by privacy commissioners about information sharing across national borders; for example, US companies processing Canadian data were subject to US law so it was not possible for the Canadian government or other bodies to guarantee the security of those data.

6. The interception of communications by state authorities was regarded as a very intrusive power which normally required judicial authorisation. The written application for judicial authorisation is put together with a great deal of care. It is made available in any subsequent court proceedings. It was for the courts to decide whether any parts of the intercept material itself should be redacted before being disclosed in the course of a prosecution. The Minister of Public Safety reports annually on the number of interceptions made.

7. Currently in Canada DNA samples were not collected upon arrest and indeed were taken only pursuant to a judicial warrant or from people convicted of certain crimes. The use of these powers was scrutinised by an advisory committee. Potential changes to DNA provisions were often a matter for public debate.

Mr Michael MacNeil, Director, Public Interest Advocacy Centre

8. The Public Interest Advocacy Centre (PIAC) was made up of various consumer groups, operated by holding consultations and making representations to the government and parliament on a variety of different subjects, including the privacy implications of legislative proposals.

9. Whilst the Charter did not articulate a specific right to privacy, section 8 (on search and seizure) was relatively well-developed in protecting privacy. Section 7 (on life, liberty and security of person) was less well-developed in this respect. In general, there was a tendency to use the Charter as a kind of 'touchstone' and the courts had said that it should inform the development of the common law. The Charter was useful because it set out a series of general privacy principles that could guide the legislative process. By contrast, specific statute such as the Privacy Act (which governed the public sector) was liable to become out-of-date and require regular amendment. Codes of conduct were probably less useful than legislation for protecting privacy because of inconsistencies in their application.

10. Turning to intercepts, the system of judicial oversight was thought to provide a greater measure of protection although this was hard to prove in practice. It was true to say that this system tended to encourage authorities seeking a warrant to make significant efforts to justify their proposed actions. The intercept material had to be disclosed once the suspect had been charged, subject to any redactions agreed to by the judge. Specially appointed representatives were able to view the redacted parts.

Roundtable Discussion at the University of Ottawa

11. The Committee held a roundtable discussion with the following people: Professor Ian Kerr (University of Ottawa); Professor Jane Bailey (University of Ottawa); Professor Valerie Steeves (University of Ottawa); Ms Stephanie Perrin (Service Canada); Ms Pippa Lawson (Canadian Internet Policy and Public Interest Clinic); Ms Heather Black (former Assistant Privacy Commissioner of Canada); and Mr Murray Long (Privacy Consultant, Murray Long and Associates).

12. In constructing the legislative framework in this area, it was important to have an overarching statement of principles setting out the importance of privacy to democratic society and providing the judiciary with appropriate language and concepts. An excellent example was Australia's privacy charter. In order to achieve this, the Canadian Charter needed to be clearer on what constitutes a 'reasonable expectation of privacy' and whether this should be understood in terms of a desirable norm rather than in terms of what people have actually come to expect, which is subject to decline. This presented problems, however, because such a concept was bound to be subjective and was likely to change (probably diminish) as technologies developed and became standard. The growing use of technologies such as radio frequency identification (RFID) and social networking sites were particularly significant in this regard. It was therefore necessary to think in advance about the acceptable uses of such technologies, including through the medium of a rigorous public policy debate, whilst also bearing in mind that certain data may yield more and different information in the future.

13. In Canada there were privacy commissioners at both federal and provincial level. The federal commissioner was an Officer of Parliament who reported to parliament annually, which provided a good opportunity to highlight the most pressing issues. However, there were very few effective sanctions available to the commissioners and there was widespread non-compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) which governed privacy in the private sector. Enforcement action did take place through the courts but this was very expensive. It was suggested that it should be made easier for private sector companies to be held to account and that the privacy commissioners should be given order-making powers. In addition, the privacy commissioners in the provinces needed greater resources if they were to engage proactively in investigations.

14. It was also necessary to tighten up the current Privacy Act (parliament was in the process of looking at it) which was weaker than PIPEDA. Unfortunately there was only sporadic interest in surveillance and data issues in parliament, although this partly reflected the fact that there was much less surveillance in Canada than in other countries such as the UK. The Committee on Access to Information, Privacy and Ethics did play an important role but tended to focus on headline-grabbing issues like ID theft, which was not a core data protection issue.

15. It was felt that public awareness of surveillance and data protection issues was episodic, partly because Canadian citizens tended to trust the government and its assertions that bringing in tighter privacy protections meant that government could not operate so effectively. There had been an outcry in 2000 when it emerged that the state held dossiers on every citizen (the Longitudinal Labour Force File), but the data sets had subsequently been decompiled and there were now more effective safeguards in place. Such episodes raised public awareness. Also, research showed that people do care about their privacy but express it differently in different contexts.

16. As for the private sector, people were generally content to provide their personal information in order to obtain store loyalty cards and so forth—indeed, this was often a highly rational process—but most of them did not necessarily consider the cumulative effect of handing over such data to a range of organisations. They did however show concern when organisations were perceived to be using data in an underhand or non-transparent manner. There was also a growing awareness that data could sometimes be used in ways which could result in discrimination against certain types of people.

17. There was further concern amongst those present about the leaching of information from the private sector to the public sector, particularly in the absence of statutory authorisation. For example, internet service providers (ISPs) shared information on child pornography with the police but these arrangements had never been validated by a transparent public policy decision and there seemed to be no 'reasonable expectation of privacy' with regard to ISPs. In this connection, there was also concern about the use of warrants to gain access to ISP records, and about the reversal of the presumption of innocence.

18. Similarly there was consternation about the flow of information (particularly health information) from the public sector to the private sector when public functions were outsourced. This was particularly worrying where foreign companies were involved. Indeed, British Columbia had amended the law so that companies holding health information have to be Canadian-controlled and all data processing must take place in Canada, in order to ensure that data are not exported abroad and then misused.

19. Turning to the issue of DNA, it was felt that the Canadian government would not be able to introduce the kind of extensive DNA database that existed in the UK because it would fall foul of the Charter and the wider privacy culture, and because of the likely cost to the taxpayer. However, the very limited database in Canada was growing through 'mission creep'.

Office of the Privacy Commissioner of Canada

20. The Office of the Privacy Commissioner of Canada was represented by Ms Jennifer Stoddart (Privacy Commissioner of Canada) and colleagues.

21. The Privacy Commissioner of Canada, an Officer of Parliament, reported directly to a parliamentary select committee rather than a minister and her budget was determined by an all-party review panel chaired by the Speaker of the House of Commons (so far, the panel had agreed to all budget requests from the Privacy Commissioner's Office). These arrangements reflected the importance of the post-holder being autonomous from the Government. Keeping abreast of technological changes was difficult but they did their best by employing two full-time technology experts to advise (it was also possible to commission external advice) and by having representation on other bodies within and outside Canada where questions of, for example, wireless technologies and CCTV were being considered.

22. Canada also had a federal Information Commissioner, who was entirely separate from the Privacy Commissioner except in budgetary terms. The two of them rarely had disagreements. It was not really important whether there were two separate commissioners (as in Canada) or one Information Commissioner fulfilling both functions (as in the UK); it was the powers and resources available to the commissioner(s) that mattered.

23. The Privacy Commissioner had been calling for reform of the Privacy Act, which was weaker and more out-of-date than PIPEDA, although this might be difficult to achieve while the government lacked a majority. PIPEDA had benefited from the history of its development, which involved making Canadian privacy protection 'adequate' in accordance with the EU Data Protection Directive. Under PIPEDA, private sector privacy disputes were increasingly being taken to the federal courts, and it would be desirable for a revised Privacy Act to make it easier to do the same in respect of the public sector. Government officials resisted strengthening the Privacy Act.

24. Reform of the Privacy Act should also cover Privacy Impact Assessments (PIAs). PIAs were currently 'encouraged' through funding mechanisms under the Treasury Board Directive, and the Privacy Commissioner was empowered to suggest changes to them which were usually accepted. However, it would be preferable for PIAs to be made a mandatory requirement and for them to be made more widely available to the public in order to inform dialogue. PIAs gave the Commissioner a window into how major government programmes worked and into proposals such as the enhanced drivers' licence scheme. It had taken a while before PIA requirements had been comprehended by agencies, and the Commissioner had developed systems for auditing and vetting agencies' PIA practices.

25. It would also be desirable for the Treasury Board definition of 'data matching' to be broadened so as to increase the inadequate scrutiny of government activity in this important area. For example, the courts had ruled that it had been permissible under the Privacy Act as currently drafted for the public not to be told that information obtained from landing cards was being matched with the employment

insurance database to ensure that unemployed people were staying in Canada and looking for jobs.

26. Canadians tended to be instinctively opposed to the collection and use of DNA along the lines of a UK-style system. The Commissioner would be particularly concerned by practices of familial analysis and the sharing of DNA profiles with countries where the data would be inadequately protected. However, there had been a gradual increase in the use of DNA in Canada and the Royal Canadian Mounted Police had pointed to the UK as a model in this regard. The defence industry was also finding new uses for DNA. Developments in forensic science acted as a driver to DNA use.

Information Commissioner of Canada

27. The current Information Commissioner, Mr Robert Marleau, had previously been the Clerk of the House of Commons and subsequently the Interim Privacy Commissioner (IPC). Like the Privacy Commissioner, the Information Commissioner was an Officer of Parliament which reinforced his independence from government and his influence with parliament.

28. There had been an inquiry in 2005, conducted by a former Justice of the Supreme Court, Gérard La Forest, into the question of whether the roles of Privacy Commissioner and Information Commissioner should be merged (as in the UK). Both Mr Marleau and Jennifer Stoddart, the Privacy Commissioner, had opposed such a merger. The inquiry had also come out against a merger because, while there was not much interest outside Ottawa in access to information, there was a strong interest in privacy (especially in light of 9/11) so a full-time Privacy Commissioner was needed. There was also a tension between the principles of privacy and access to information—albeit a generally positive tension—so it was preferable to have two separate commissioners representing people's rights in each area. Both commissioners should share a mandate to educate the public.

29. Where privacy and public access were both involved in an issue, Mr Marleau thought that one should err on the side of privacy. In fact, there had only been one court case in 25 years in which the two conflicted, and public access had lost out. Since 2005, there had been a parliamentary committee on Access to Information, Privacy and Ethics. It was a useful committee, providing greater scrutiny of freedom of information and privacy protection issues. The committee was able to subject bills to pre-legislative scrutiny, although it had not yet done so. The Information Commissioner could give to the committee 'performance report cards' on government departments.

30. As IPC, Mr Marleau had faced two key issues: CCTV and ID cards. His predecessor, George Radwanski, had campaigned strongly against CCTV and brought a major case in British Columbia. However, the case was becoming very expensive and would probably have been lost on grounds of jurisdiction, so Mr Marleau decided to drop the action. He reached agreement with the police that guidelines on CCTV use should be formulated, and these were published in 2006. This informal, non-statutory approach was preferable to passing detailed legislation which might result in drawn-out court cases. Similarly, the large number of CCTV cameras in the UK would not necessarily be a problem provided that there were clear guidelines and policy statements, as well as maximum transparency.

31. Mr Marleau had taken a very firm stand against ID cards when he was IPC because there had been insufficient justification for introducing them. The issue

had arisen again recently with enhanced drivers' licences which would, using radio-frequency identification (RFID) technology, speed up border crossings into the USA. Not only might this scheme be a first step towards a national identity card, there was also concern about sharing personal information with the USA (which could potentially turn that information into a commercial product) and about possible data mining.

Mr Larry Kearley, Vice-President, Canadian Access and Privacy Association (CAPA)

32. The Canadian Access and Privacy Association (CAPA) was a national non-profit organisation which aimed to promote knowledge and understanding of access and privacy laws and experiences in Canada. It dealt with both the three levels of government (federal, provincial, local) and the private sector.

33. The Canadian Charter and the European Convention on Human Rights had much in common. They were both quite vague, unlike the American Bill of Rights, but this allowed a measure of flexibility which enabled them to accommodate changes in society and so forth. However, it was noteworthy that neither document was specifically aimed at surveillance or data issues.

34. There were however significant differences between the UK and Canada in terms of levels of surveillance and data collection. For example, the UK was well-known as a CCTV society, whereas Canadians were very suspicious of surveillance cameras—perhaps because of the lower crime rates and risks of terrorism compared with the UK and the USA, although Canadians were concerned about crime and child pornography. In addition, it was significant that the UK had only one privacy/information commissioner for 60 million people, whereas the Canadians had numerous privacy and information commissioners for just 30 million people.

35. A potential danger facing all countries was the increase in cross-border information flows. There were particular dangers from outsourcing personal data to countries such as India, where privacy protections tended to be weaker. Moreover, many of these high-risk countries suffered from terrible poverty so the chances of identity theft were much higher than elsewhere.

36. The effective protection of privacy required a mixture of laws, codes of practice and privacy-enhancing technologies (PETs). Members of the public could use encryption and anonymity devices, but only a minority would be able to benefit from these unless they were built into software. Chief Privacy Officers could be useful but in the private sector they saw their primary role as protecting their companies rather than limiting the invasion of customers' privacy. Privacy Impact Assessments were also a good idea, but so far were used mainly in the private sector, and for risk assessment.

Madam Justice Rosalie Abella, Supreme Court of Canada

37. The Canadian Charter of Rights and Freedoms had had a very significant impact on the country's jurisprudence. The Charter contained both 'freedom from …' rights—similar to those contained in the US Bill of Rights—and equality rights, which had gained currency after the Second World War.

38. There had been a Bill of Rights (enacted in 1960) before the Charter, but judges had not generally been comfortable with the idea of enforcing rights and pronouncing on state-citizen relations. Once the Charter was enacted in 1982, the Supreme Court increasingly took up the concept of rights and in the 1990s encountered significant hostility from the media and the public over its attempts to

uphold the rights of the accused and of gay people. In the current decade, the Court had perhaps retrenched from some of the more radical decisions of the 1990s. Crucially, it was possible for parliament, *in extremis*, to overrule the court's interpretation of the Charter.

39. Most significant privacy rulings of the Supreme Court had been concerned with criminal issues, although there had been a very important ruling establishing a woman's right to choose to have an abortion. A recent ruling on informational privacy in *R. v Tessling* [2004] had concerned airborne Forward Looking Infra-Red cameras (FLIRs) heat-sensor devices that could help to search for marijuana cultivation in buildings and whether the police needed a warrant to operate them. The lower courts had ruled that a warrant was needed, but the Supreme Court overturned that decision. An important issue was what constituted a 'reasonable expectation of privacy'. This should always be a contextual assessment because in certain circumstances—such as when you cross a national border—you inevitably have a reduced expectation of privacy. Indeed, the courts had upheld the idea that people have a reduced expectation of privacy in certain places. However, even with a contextual assessment the 'reasonable expectation' formula was ambiguous because of the different expectations of different kinds of people: for examples, whites, ethnic minorities or gay people.

40. The British courts had been robust in upholding citizens' rights, for example in the rulings on the detention of foreign terrorism suspects and control orders. It also appeared that privacy rights in the UK were increasing—the Naomi Campbell case being a prime example—but they were still not well-defined. However, it would not necessarily be advisable for a tort of privacy to be developed in the British courts.

Mr Ken Anderson, Assistant Commissioner (Privacy), Office of the Information and Privacy Commissioner of Ontario

41. In Ontario there was just one commissioner responsible for both information and privacy (Dr Ann Cavoukian), but she had two assistant commissioners—one dealing with information and the other with privacy. With 93 employees in total, the Office was very well staffed.

42. Whilst the Assistant Commissioner (Information) focused predominantly on tribunals, Mr Anderson spent 90 per cent of his time on advocacy and research. A key role of the Commissioner's Office was to influence politicians and police chiefs on privacy and access issues, for example through policy briefings, meetings and communications with the media. The Office also worked with interest groups and the Human Rights Commission. It aimed to gain leverage by working with players in various fields to make systematic changes; for example, the Office had worked with Facebook (a popular social networking website) to enhance privacy and online safety. At the international level, the Office had discussed with the USA's Department of Homeland Security matters such as the information held on passengers taking cross-border flights.

43. Privacy Impact Assessments (PIAs) could be useful but they varied widely in quality. It was not sufficient simply to produce a template PIA and leave it at that, because constant thought and improvement were required. In Ontario, PIAs were used extensively in the healthcare field—especially by large organisations—but should also be extended to other sectors. It was sometimes desirable to use PIAs to do a "snapshot" of existing policies; for example, this might be a good way of assessing the use of CCTV in the UK.

44. CCTV was not as popular in Canada as it was in the UK, although around 70 per cent of Canadians supported its use on public transport (a figure which tended to rise to 80 per cent or more if there had been a recent criminal incident). All privacy commissioners in Canada produced guidelines on the use of CCTV. The Office worked with the police to limit the collection of images. The latest suggestion for enhancing people's privacy was to encrypt images of people caught on CCTV (particularly where the camera's primary purpose was something other than crime prevention) in order to anonymise them. Images could subsequently be unencrypted where necessary, for example if a crime was committed.

45. In Canada, the rules governing the collection and retention of DNA samples were set out in the Criminal Code, which had the force of statute. The police were able to take DNA samples in certain specified circumstances, although generally they had to apply to the courts for a warrant. DNA samples could also be taken from volunteers, but there were no provisions in the Criminal Code governing retention in such circumstances. Canada had no equivalent of the UK's National DNA Database Ethics Committee.

UNITED STATES OF AMERICA

Mr Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, IDAnalytics

46. IDAnalytics was a company that collected personal data in order to deliver accurate predictions of the likelihood of identity risk associated with applications for credit. Having collected the available data, the company processed them (through a series of complex computer programmes) to produce a 'score' which was given to clients; the data themselves were not shared with clients so there was minimal risk of data being misused.

47. The kind of assessments provided by IDAnalytics were needed because business nowadays operated in a more impersonal and less 'one-to-one' way than in the past. It was desirable for trusted parties to hold large amounts of data which could be used to provide a conclusion or summary to bank and other organisations, because this kept the data secure and removed the need for large amounts of information to be disseminated. In addition, holding data could help to protect people's privacy by preventing fraud and identity theft, which in itself was a social good. Data mining could also be beneficial, but it was important to avoid mission creep. It was difficult to determine where privacy protection ended and identity verification began.

48. The proliferation of chief privacy officers was a relatively new phenomenon. The role involved ensuring compliance with relevant laws and regulations and adherence to the company's or organisation's privacy policy. Chief privacy officers also served to provide an interface with members of the public over, for example, access to information requests.

Centre for Democracy and Technology

49. The participants from the Centre for Democracy and Technology (CDT) were: Mr Greg Nojeim (Senior Counsel and Director of CDT's Project on Freedom, Security and Technology); Mr Ari Schwartz (Vice President and Chief Operating Officer); and Professor Peter Swire (Policy Fellow).

50. In addition to the US Bill of Rights, the US Constitution provided an architecture of checks and balances that enabled any excesses by government

departments to be discovered. There was nonetheless a need for the executive to exercise self-restraint when it came to the invasion of privacy, for example through the use of due diligence checklists which had the potential to cool the initial enthusiasm about a particular idea by highlighting possible problems and downsides. Privacy Impact Assessments (PIAs) were useful in this regard, because they were made public and therefore increased transparency and forced departments to answer concerns. However, if departments were determined to press ahead with particular schemes, it was unlikely that PIAs could make much difference.

51. The Clinton presidency, taking its lead from Canada and the private sector, had viewed PIAs as a best practice tool. Since 2002 they had been required in certain circumstances but they tended to be very variable in quality, and some amounted to little more than 'box-ticking' exercises. For example, the PIA of the new passport system had been only one page in length. However, as part of the reauthorisation of the E-Government Act, further consideration was being given to how PIAs ought to be conducted. The Office of Management and Budget (OMB) in the executive branch was drafting a 'best practice' manual on PIAs.

52. There were no privacy commissioners in the USA and, while it would be desirable to introduce them, it was in reality necessary to work with the existing bodies such as the Federal Trade Commission (FTC). The CDT sometimes took winnable cases to the FTC on issues such as spyware.[234] There was also a Privacy and Civil Liberties Oversight Board which was tasked with advising the President in the context of the fight against terrorism, although it had initially been seen as too close to the White House. The Board had now been re-modelled and was likely to be more independent, with its members having to be approved by the Senate, but it currently had neither members nor funding. It would probably not start operating until the next President took office.

53. The current administration, with its overwhelming focus on national security, was thought to have neglected the issue of personal privacy. In particular there had been widespread abuse of so-called National Security Letters (NSLs) which enabled the FBI, without obtaining a court order, to require a particular entity or organisation to hand over various records and data pertaining to individuals. It was particularly notable that NSLs could be used to obtain personal data from overseas that were held by American companies. Moreover, the FBI was entitled to forbid an organisation subject to an NSL from telling anyone about the demand. Congress had put in place an audit system which had picked up some of the abuses as well as ascertaining that NSLs had been used hundreds of thousands of times. The government had subsequently issued better-practice guidelines but it was not certain how far they were being followed.

54. There was a more general concern that the protections provided by the 4th Amendment (protection from unreasonable search and seizure) were getting progressively weaker. First, the government had undermined the principle that warrants were required for searches and seizures, often by classifying investigations as foreign intelligence gathering rather than regular law enforcement, thus bypassing traditional 4th Amendment protections. Second, the Supreme Court had become chary of the 4th Amendment and had made it less useful. Access to communications data was not covered by the Amendment because the 'search and

---

[234] Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

seizure' pertained to internet service providers rather than individuals or their homes.

55. Another key concern was the REAL ID Act, which provided for homogenised federal driving licences. There was considerable opposition to this scheme from the states and the public because it federalised something that had been under state control. Moreover, it was easier for the federal government than state governments to share people's personal data, and federal law trumped any privacy requirements in state constitutions.

American Civil Liberties Union

56. The participants from the American Civil Liberties Union (ACLU) were: Mr Wes Macleod-Ball (Chief Legislative and Policy Counsel); Ms Michelle Richardson (Legislative Counsel); and Mr Jay Stanley (Public Education Director, Technology & Liberty Program).

57. Attitudes to privacy did not break down on political lines: just as many libertarian Republicans as Democrats were concerned about the erosion of privacy, so there was a great opportunity to make progress. Whilst national security remained a high priority amongst Americans, a growing number of them were becoming increasingly concerned about privacy issues although they did not always understand what happened to their data in terms of profiling and sharing. The ongoing challenge was to show people how they could be affected by certain initiatives—especially the PATRIOT Act and programs similar in means and ends to the now defunct Total Information Awareness (TIA) Program (such as the one that the NSA seems to be pursuing)—in practical, concrete ways. The ACLU strongly encouraged members of the public to put any concerns to their congressmen, which was often more effective than direct lobbying or litigation. The media also played a hugely important role.

58. It was essential that controversial legislation such as the PATRIOT Act should contain sunset clauses, because Congress was generally loath to revisit legislation unless they had to do so. It was perfectly possible for law enforcement agencies to adjust to changes in their powers.

59. The excessive collection of personal data by the government was thought to be a breach of privacy in itself, regardless of whether those data were subsequently used for malign purposes. There was particular concern about the REAL ID Act which was seen as a mechanism for introducing a *de facto* national identity card. Not only were the ACLU concerned about a potential shift towards a 'checkpoint society' where citizens have to show their papers or identification on a regular basis, they were also worried about the database behind the cards because the aggregation of data could be very problematic given the potential insecurity of the database. There was further concern about the private sector's realisation that collecting their customers' data could be commercially advantageous, particularly since the government could potentially seize or buy those data.

60. The collection and retention of DNA samples was another pressing issue in the USA. Almost all states required convicted felons to be on a DNA database, but a battle was now being fought over whether arrestees should also be added as in the UK. However, unlike in the UK, most states pursuing this path were also specifying that an arrestee's sample should be removed if he or she was not charged or convicted of an offence.

Roundtable Discussion at the Electronic Privacy Information Center

61. The Committee held a roundtable discussion at the Electronic Privacy Information Center.

62. The events of 9/11 had resulted in the prioritisation of national security, often at the expense of privacy and civil liberties. This went well beyond the USA PATRIOT Act which, although very important in itself, had assumed a symbolic importance and had been kept in the public eye by the need to renew the sunsetted provisions. But just as civil liberties were coming increasingly under threat in the name of national security, the Supreme Court had arguably moved away from protecting such liberties. This meant that advocacy groups had become more important than ever. Technology helped them to organise public campaigns quickly and effectively and they continued to be active on Capitol Hill and in the media.

63. The National Commission on Terrorist Attacks ('the 9/11 Commission') had emphasised that new security measures needed to be counter-balanced by oversight. Chief Privacy Officers were an important part of this oversight process and had made an effort to 'reach out', but they had to oversee a huge policy area—particularly Hugo Teufel in the Department of Homeland Security (DHS)—and were not genuinely independent (those in the DHS and the Department of Justice were political appointees). Moreover, PIAs were not as effective as they could be: the statutory requirements were minimal; they were only effective when the organisation in question was committed to them; they were sometimes conducted after the scheme in question had already been implemented; and the sheer volume of them often diluted the impact of even the most important ones.

64. There were big cultural differences between the USA and the UK in terms of public attitudes towards CCTV. After 9/11, there had been proposals to create a UK-style CCTV system in the USA but these had been met by serious concerns from both sides of the political spectrum. The biggest driver behind CCTV in Washington DC was crime rather than terrorism, and CCTV images were generally only viewed in the course of investigating a specific crime. There were more cameras in New York City, where Mayor Michael Bloomberg had proposed a security system similar to the 'ring of steel' around the City of London. It was notable that the Department of Homeland Security (like the Home Office in the UK) encouraged the installation of CCTV by offering funding to local councils.

65. There was a very real threat of 'ubiquitous surveillance' in the future, for example if CCTV cameras were linked into Google's 'Street View' product. Further threats were presented by potential technological developments which would, among other things, make CCTV cameras much harder to spot. The current legislation (e.g. the Video Voyeurism Protection Act 2004) and the common law provided inadequate protection against these threats. In light of this, and the fact that no challenges to CCTV had so far been made under the US Constitution, it was necessary to promulgate a set of principles governing the use of CCTV. The concept of a 'reasonable expectation of privacy' could be useful, but it could also lead to an inexorable spread of CCTV in high crime areas (because of lower resistance to CCTV amongst the local community) and the automation of policing.

66. It was possible that Congress would only be prompted to take action by a high-profile Supreme Court case, perhaps involving a celebrity. This reflected the fact that it was often necessary to have some 'trigger' event before the exertion of central control became acceptable to the public or palatable to politicians. It was

also necessary for the civil rights community to engage with CCTV and related issues, moving on from the issues of the 20th century and confronting the new challenges presented by technology. Such an engagement with the issues would increase the pressure for action.

67. Public opinion in the USA was generally against identity cards. The REAL ID Act (see paragraph 55 above) had never been properly debated in Congress and there was now a considerable public backlash against it. Around 20 states had passed legislation opposing the Act and there was an ongoing stand-off between the states and the Department of Homeland Security. There was also a dispute about who should pay for the scheme. The main problem in many people's eyes was the database behind the identity documents. It would be preferable (and possible) to design a system whereby only the individual could 'unlock' information about themselves. This would avoid the dangers of having an enormous database and remove the temptations of 'function creep'. However, even revealing a name would enable law enforcement officials to conduct further searches, so it might be desirable to have a system whereby individuals could establish their entitlement to something but without revealing their identities.

68. The courts had upheld the DNA database on the basis that convicted felons have a lower expectation of privacy than others. However, law enforcement agencies were constantly pushing the boundaries; for example, the FBI had proposals on familial searches and partial matches (which could well fall foul of the courts) and there was a suggestion that some police forces had taken to following suspects in an attempt to obtain an item which might yield a DNA sample and thus link the suspect to the scene of a crime.

Office of Representative Jerry Nadler

69. In the absence of Representative Jerry Nadler, the Chairman of the House Judiciary Subcommittee on the Constitution, Civil Rights and Civil Liberties, the Committee met with his Chief of Staff, Mr David Lachmann, and his Legislative Counsel, Ms Carole Angel.

70. There had been many abuses of National Security Letters (NSLs) since the USA PATRIOT Act had been passed. A bill put forward by Representative Nadler would restore many of the pre-PATRIOT controls on the issuance of NSLs, but the administration was resisting the bill because it felt that the issue could be dealt with by means of administrative changes. The bill did not have the Republican support it needed to pass the House, partly because the law enforcement agencies had said that they felt that the proposed changes to the current regime would stop them doing their jobs properly. Nonetheless, there was considerable momentum behind the aims of the bill.

71. Chief Privacy Officers (CPOs) could be a valuable asset—indeed, the first CPO at the Department of Homeland Security, Nuala O'Connor Kelly, had been highly respected—but generally they lacked the degree of independence that CPOs across the world tended to have. It would therefore be desirable to bring in a new generation of more independent CPOs.

72. The REAL ID Act was a big issue at state and local level and there was in general a visceral public opposition to ID cards in the USA. Indeed, the federal government was offering grants to encourage reluctant states to implement the Act. There were also constitutional concerns regarding requirements placed on immigrants and visitors, and issues of due process. A recent US Supreme Court case on voters' ID had raised issues about impediments to voting and whether a

requirement for ID was an impediment if the ID did not have to be paid for by the voter.

Federal Trade Commission

73. The Committee met with Commissioner Jon Leibowitz and colleagues.

74. The Safe Harbor arrangement provided a way for US companies to comply with the EU Data Protection Directive. So far, the Federal Trade Commission (FTC) had not dealt with any problems or complaints under the arrangements and, whilst they were by no means perfect, this was taken to be an indication of adequacy. Data flows across national boundaries were now very common and it would be desirable for different countries to agree common standards; however, this would be very difficult in practice.

75. The FTC could intervene if a US company holding data on UK citizens unlawfully shared or lost that data. However, if those data were demanded by a US law enforcement agency (for example through a National Security Letter) then the FTC was not empowered to do anything. Indeed, whilst the FTC liaised with government on a departmental or agency basis, it did not have any jurisdiction over other governmental organisations.

Department of Homeland Security

76. The participants from the Department of Homeland Security (DHS) were: Mr Hugo Teufel III, Chief Privacy Officer and Chief Freedom of Information Act Officer; Mr John Kropf, Deputy Chief Privacy Officer; and other members of staff.

77. Privacy Impact Assessments (PIAs) were required in certain circumstances under section 208 of the E-Government Act 2002, although the DHS also carried out some PIAs not required by statute (e.g. the PIA on full body imaging). The DHS PIAs were based on the eight 'fair information principles' which in some ways resembled the principles in the UK Data Protection Act. PIAs were useful because they forced the DHS to think very carefully about privacy and how to build in privacy safeguards. The system also had 'teeth' because, unlike in Canada, PIAs were linked to funding. It was important that PIAs should be made public so as to inform people—and perhaps give them confidence—about the government's activities.

78. A handful of government departments, including the DHS, had been required to employ Chief Privacy Officers (CPOs) since the 9/11 Commission reported. The different CPOs worked very closely together. CPOs were desirable because it was better to counsel and advise departments from the inside, rather than have an independent privacy officer (such as Richard Thomas) criticising from the outside. However, it was true to say that CPOs varied in their approaches depending on how seriously they were taken and how independent they were. It might be advisable for the United Kingdom to use departmental CPOs.

79. It was important to note that key decisions to invade individual privacy were taken by legislators, not by government agencies and their employees—it was up to Congress to scrutinise proposals and approve or disapprove them. The DHS talked informally to Congress and testified as part of the oversight process, but the CPO served the President and the Secretary of the Department of Homeland Security so would not express views to Congress that disagreed with the President's policies. However, he did see it as his responsibility to speak candidly within the DHS itself.

Mr Ken Mortensen, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

80. It was important to have an officer focused on privacy issues—indeed, the job of the CPO was to protect the public from the Department of Justice (DoJ). Unlike the CPO in the DHS, the CPO in the DoJ oversaw civil liberties issues but not freedom of information. He was also more integrated into the rest of the department so tended to be present during the policy development phase, whereas the DHS CPO had an independent office.

81. The Office of Legal Counsel (OLC) within the DoJ consisted of lawyers tasked with determining the meaning of existing laws and setting out the ways in which the executive could or could not act. The courts paid heed to OLC opinions. Most government agencies also had a general counsel who was able to ask the OLC to clarify any points of legal uncertainty.

82. Until recently in the United States, it had only been possible to take DNA samples from convicted criminals, but law enforcement agencies were now permitted to take samples from arrestees for purposes of identification. The samples were to be kept for 100 years, as with fingerprints, and there was a possibility of a certain amount of 'function creep'. Fingerprints and basic biographical information could be shared across law enforcement agencies but there were severe restrictions on sharing with other bodies. There was a mechanism for data matching across states for criminal justice-related purposes as well as for some non-criminal justice purposes where access was possible (for example criminal record checks for employment).