House of Commons
Home Affairs Committee

A Surveillance Society?

Fifth Report of Session 2007–08

Volume I

Report, together with formal minutes

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

HC 58-I
[Incorporating HC 508-i–iv, Session 2006–07]
Published on 8 June 2008
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The Home Affairs Committee

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

Current membership

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

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

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

Powers

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

Publication

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

Committee staff

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

Contacts

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

Contents

Report

Summary

In the design of its policies and systems for collecting data, the Government should adopt a principle of data minimisation: it should collect only what is essential, to be stored only for as long as is necessary.

We call on the Government to give proper consideration to the risks associated with excessive surveillance. Loss of privacy through excessive surveillance erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state. The decision to use surveillance should always involve a publicly-documented process of weighing up the benefits against the risks, including security breaches and the consequences of unnecessary intrusion into individuals' private lives.

Our Report sets out a series of ground rules for Government and its agencies to build and preserve trust. Unless trust in the Government's intentions in relation to data collection, retention and sharing is carefully preserved, there is a danger that our society could become a surveillance society.

The potential for surveillance of citizens in public spaces and private communications has increased dramatically over the last decade, making it possible for what the Information Commissioner calls "the electronic footprint" we leave in our daily lives to be built up into a detailed picture of our activities. This has prompted growing concern about a wide range of issues relating to the collection and retention of information about individuals.

The commercial sector has driven a great many of the developments in this area, recognising the competitive advantage that information about customers can bring when used to target marketing and design personalised services. Government has also sought to harness this capability, to meet public expectations for similarly tailored and convenient services. Advances in technology have influenced the public's ideas about what it can deliver for the prevention and investigation of crime. The outcome has been the collection and sharing of increasing amounts of personal information.

The collection of personal information by public and private sector bodies can have clear benefits for the consumer, the patient and the recipient of public sector services. But it also involves significant risk. Mistakes in or misuse of databases can cause substantial practical harm to individuals—particularly those who have little awareness of or control over how their information is used.

The Government should make full use of technical means of protecting personal information and preventing unwarranted monitoring of individuals' activities. But safeguards are as much a matter of policy and protocol as of technology: the Government should also carry out rigorous risk analysis of any proposal to establish major new databases or other systems for collecting data, take full responsibility for protecting personal information, and ensure that its policies and procedures in relation to data collection and storage are as transparent as possible.

We examined aspects of the Home Office's responsibilities in relation to the collection and sharing of personal information—including CCTV or video surveillance, identity cards

and the National DNA Database—and considered how information collected in other public and private sector databases might be shared for use in the fight against crime. We recommend that the Home Office exercise restraint in collecting personal information, and address the question of whether or not surveillance activities represent proportionate responses to threats of varying degrees of severity.

Ground rules for Government

Rules for Government as a whole

The Government should give an explicit undertaking to adhere to a principle of data minimisation and should resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or to implement proposals for increased surveillance, should be based on a proven need.

The Government should take responsibility for safeguarding the personal information it collects and should exercise this responsibility before collection takes place: when it is possible by obtaining consent for collecting and processing data, and when it is not possible by providing an explanation.

The Government should hold information only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes as well as for service delivery it should normally be anonymised and retained only for a previously specified period.

Every system for collecting and storing personal information should be designed with a focus on security and privacy. This process should involve planning not only the technical aspects of access to systems but also the staff management protocols for access and information-handling.

The Information Commissioner should lay before Parliament an annual report on surveillance. The Government should make a formal response to his report, also to be laid before Parliament.

Rules for the Home Office

The Home Office should explicitly address these questions in every proposal for extending or changing its powers and functions with regard to the collection and use of personal information: in the fight against crime: where should the balance between protecting the public and preserving individual liberty lie? How should this balance shift according to the seriousness of the crime? What impact will there be on the individual and on our society as a whole?

The Home Office should not routinely use the administrative information collected and stored in connection with the National Identity Register to monitor the activities of individuals.

The Home Office should maintain plans for securing the National Identity Register databases, and contingency plans to be implemented in the event of a loss or theft of biometric information from its databases.

The Home Office should take every opportunity to raise awareness of how and why the surveillance techniques provided for by the Regulation of Investigatory Powers Act might be used, and should keep under review the effectiveness of the statutory oversight of RIPA powers.

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.

1 Introduction

Outline of the Committee's inquiry

1. In March 2007 the Home Affairs Committee launched a wide-ranging inquiry into the growth of public and private databases and those forms of surveillance directly relevant to the work of the Home Office. We decided to consider the following key issues:

- Access by public agencies to private databases
- Data-sharing between government departments and agencies
- Existing safeguards for data use and whether they are strong enough
- The monitoring of abuses
- Potential abuse of private databases by criminals
- The case for introducing privacy impact assessments
- Privacy-enhancing technologies
- Profiling

2. The growth of the so-called "surveillance society" has already been subject to a detailed and wide-ranging inquiry by the Surveillance Studies Network, carried out at the request of the Information Commissioner. Our aim was not to duplicate that work but rather to build on it in exploring the large strategic issues of concern to the general public.

3. The boundary between what is a legitimate tool in the fight against crime, and what constitutes an unacceptable intrusion into an individual's privacy is a fraught and disputed one. We set out to examine the evidence with a view to proposing ground rules for Government and its agencies.

4. We received over 60 memoranda and took oral evidence on six occasions. We began by taking evidence from the Information Commissioner and went on to hear from witnesses on matters such as the collection and use of personal information by private sector organisations, the technological and social developments which have affected—or which are likely to affect—how personal information is stored and shared, and the impact of various kinds of surveillance on privacy and individual liberty. We took further evidence on government databases and information-sharing, and on surveillance and the fight against crime; and we completed our inquiry by hearing from the Home Office. A list of those who gave oral evidence is annexed.

5. We visited the USA in connection with our inquiry, holding meetings with—amongst others—the Department of Homeland Security, the Department of Justice, Microsoft, the American Civil Liberties Union and Senator Joe Lieberman in Washington DC, Governor Martin O'Malley and State staff in Annapolis, Maryland and Mayor Sheila Dixon and City staff in Baltimore, Maryland. We are grateful to all of those who made time to meet us and extend our thanks to HM Ambassador Sir Nigel Sheinwald KCMG, Alan Charlton CMG,

CVO, then Deputy Head of Mission, and all of those Foreign and Commonwealth Office and locally-engaged Embassy staff who assisted us.

6. During our inquiry we also held an informal meeting with a high level expert committee commissioned by the Government of the Netherlands to examine the way in which intelligence and police organisations collect data from external databases and share it with their partners.

7. We record our thanks to our Specialist Adviser, Professor Nigel Gilbert of the University of Surrey and the Royal Academy of Engineering.

Background to the Committee's inquiry

8. Surveillance plays a part in the life of the individual and in society as a whole that can often go unnoticed. It can also, however, be the source of deeply-felt unease and concern. A perception of the growth of surveillance—in particular the collection, storage and use of personal information—as an increasingly important part of the Government's policy in tackling crime, managing borders and delivering public services, lay behind our decision to undertake this inquiry. We examined Home Office responsibilities—such as identity cards, the National DNA Database and CCTV—in this context.

Benefits and risks of surveillance

9. We have examined the benefits of surveillance in terms of public safety and public services, and the risks in terms of the consequences of mistakes, mis-identification, and loss of sensitive information. We found that the way in which the balance between benefit and risk is negotiated has potentially profound implications. Privacy plays an important role in the social contract between citizen and state: to enjoy a private life is to act on the assumption that the state trusts the citizen to behave in a law-abiding and responsible way. Engaging in more surveillance undermines this assumption and erodes trust between citizen and state. In turn such an erosion of trust—with the citizen living under the assumption that he or she is not trusted by the state to behave within the law—may lead to a change in the reaction of the citizen and in his or her behaviour in interactions with other citizens and the Government.

10. This is not to say that the Government should not seek to prevent crime or to enforce the law but to draw attention to the danger of giving the impression through intensifying surveillance—even if it is a false impression—that everyone is a suspect. More than simply a matter of the Home Office and Government in general setting the right technical or bureaucratic standards, the collection and storage of large amounts of personal information which may be used to build up a picture of an individual's activities can ultimately affect the nature of the relationship between the individual and the Government and in turn the nature of the society in which we live.

HMRC data loss and recording of conversations at HMP Woodhill

11. Any sense that ours was a purely academic inquiry was dispelled by great public concern caused by the loss of child benefit records by Her Majesty's Revenue and Customs (HMRC) in October 2007. The legitimacy of the state's control of data has also been called

into question in the reporting of allegations that conversations between Sadiq Khan MP and a constituent of his who had been detained in HMP Woodhill, had been subject to covert recording in May 2005 and June 2006. The Government is itself now engaged in several reviews of the security of personal data and systems for sharing it, and Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner, has carried out an inquiry into the circumstances relating to the HMP Woodhill case.

Our Report

12. We have begun by setting out a series of steps which the Home Office in particular and the Government more generally should take to curb unnecessary surveillance, protect the public against the loss of personal data, and maintain the trust of those individuals whose sense of privacy and individual liberty underpins the relationship between citizen and state in our society.

13. In the next section we outline the broad view we have taken in relation to a working definition of surveillance. We go on to examine the growth in surveillance and the potential for surveillance and to explore some of the factors which have contributed to such a growth. We then look at the implications of this trend in terms of the benefits and risks to the individual and wider society, and the safeguards in place to minimise these risks. We go on to consider these issues in the context of particular Home Office responsibilities and the fight against crime in general.

14. **We reject crude characterisations of our society as a surveillance society in which all collections and means of collecting information about citizens are networked and centralised in the service of the state. Yet the potential for surveillance of citizens in public spaces and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the Government's intentions in relation to data and data sharing is preserved. The Home Office in particular and Government in general must take every possible step to maintain and build on this trust: our Report provides a starting point.**

2 Surveillance in context

What do we mean by surveillance?

15. For the purposes of this inquiry we have used surveillance as a term that encompasses not only the use of monitoring and recording technology but also the creation and use of databases of personal information and the record of our communications in the digital age. The Information Commissioner has called this "the electronic footprint which people leave in their daily lives":

> Every time you click your mouse, you make a phone call, use a payment card, drive your car … there is potential surveillance there.[1]
>
> Our transactions are tracked, our interactions identified and our preferences profiled—all with the potential to build up an increasingly detailed and intrusive picture of how each of us lives our life.[2]

16. In autumn 2006, the Information Commissioner asked the Surveillance Studies Network[3] to produce a report on the 'surveillance society'. The Network illustrated its research by means of a scenario, a 'week in the life' of an imaginary family in 2006, which it followed through to show how surveillance would impinge on such a family in the year 2016.[4]

17. The Information Commissioner told us that in asking the Surveillance Studies Network to produce its report, his Office was to a large extent "trying to create a wake-up call" by posing the question:

> are we moving towards some sort of surveillance society, where technology is extensively and routinely used to track and record our activities and our movements?[5]

The growth of surveillance potential

Databases

18. Work carried out by the Surveillance Studies Network and the Royal Academy of Engineering amongst others has pointed to a rapid growth in the range and reach of various methods of surveillance. According to the Surveillance Studies Network, "the foundation for all new surveillance technologies is the database" and "huge stores of

1 Q 1 (Richard Thomas)

2 Ev 196

3 a non-profit organisation dedicated to the study of surveillance in all its forms, and the free distribution of scholarly information

4 Surveillance Studies Network, *A Report on the Surveillance Society, revised with a new postscript*, March 2007

5 Q 1 (Richard Thomas)

personal data held on ordinary people are now central to both private businesses and public services". [6]

Data collection in the private sector

19. In the private sector databases are created, maintained and used by—amongst many others—banks and building societies, credit reference agencies and retailers which run loyalty or reward schemes. The scale of this data collection and storage has increased greatly in the last decade.

20. Paying for goods with debit or credit cards creates what the Royal Academy of Engineering calls "a rich trail of information about purchases".[7] There were 4.9 billion debit card purchases in 2007, an increase of 9% on 2006, and internet card payments rose nearly four-fold over the last five years, to £34 billion.[8]

21. The Financial Services Authority says that "If you're an adult living in the UK, it's almost certain your name and details are held in the files of the three main credit reference agencies".[9] An individual's credit report or credit file contains public record information such as details held on the Electoral Roll and any court judgments or records of bankruptcy, details of current credit agreements and agreements arranged over the past six years, and details of other credit checks.

22. The largest customer loyalty or reward scheme in the UK is Nectar, run by Loyalty Management Group (LMG). LMG says that approximately 50% of all UK households participate in the programme and that nineteen Nectar cards are swiped every second of the day.[10]

23. When consumers register for the Nectar scheme they are asked for contact details, lifestyle information and other details for security checks. When they use their cards, Nectar collects the date, location and total value of the transaction.[11] Tesco collects this information and the details of each purchase made by customers who participate in the Tesco Clubcard loyalty scheme. The information is held for two years before being anonymised so that it is not attributable to an individual Clubcard user.[12]

Telecommunications and the internet

24. According to the Office for National Statistics, use of information and communications technology (ICT) has grown rapidly in the last decade:

---

6 Surveillance Studies Network, *A Report on the Surveillance Society: Public Discussion Document* (September 2006), p 5

7 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 36

8 APACS, *Key Facts and Figures: plastic cards and how we used them in 2007*. Available at www.apacs.org.uk

9 Financial Services Authority, *Money Made Clear*, available at: http://www.moneymadeclear.fsa.gov.uk

10 Loyalty Management Group, "About LMG: who we are". Available at: http://www.loyalty.co.uk/about.html

11 Q 118 (Martin Briggs)

12 Q 124 (Nick Eland)

> Although digital technology is relatively new, it is already approaching the near universal levels of use of older technologies, such as analogue television or the telephone.[13]

Household internet access, for example, grew from 10% in 1998–99 to 55% in 2005–06 and rose to 61%—over 15 million households—in 2007. Between 1996–7 and 2005–06 the proportion of UK households owning a mobile telephone rose from 17% to 79%.[14] Research carried out by the Oxford Internet Institute found that households in Britain have rapidly moved to broadband internet access: of households with internet access, the proportion using a broadband connection rose from 19% in 2003 to 85% in 2007.[15]

25. Growth in these and other forms of electronic communication has increased the capacity of service providers to collect, store and use information about individuals' activities. For example, data from communications traffic can help to locate mobile telephones and catalogue website visits. Providers use such data for a variety of reasons, including billing, network management and prevention of fraud.

Data collection in the public sector

26. A strategy published by the Cabinet Office in 2005, *Transformational Government: enabled by technology*, set out the Government's intention to harness the kinds of opportunities provided by technology and used in the private sector to tailor services and marketing to meet customers' needs and increase efficiency:

> The specific opportunities lie in improving *transactional* services (e.g. tax and benefits), in helping front line *public servants* to be more effective (e.g. doctors, nurses, police and teachers), in supporting effective *policy outcomes* (e.g. in joined-up, multi-agency approaches to offender management and domestic violence), in reforming the *corporate services* and *infrastructure* which government uses behind the scenes, and in taking swifter advantage of the *latest technologies* developed for the wider market.[16]

27. In line with the objectives set out in this strategy, the Government's use of databases has become more ambitious in recent years. There are three projects that are especially notable, owing to the sensitive nature of the information to be collected or collated on new or adapted databases. The NHS Care Records Service aims to provide a nationally available lifelong patient record in order to support the delivery of care to patients and the secondary analysis and reporting of information for a variety of purposes such as healthcare planning and commissioning, clinical audit, research and clinical governance.[17] We discuss health-related databases in more detail below at paragraph 86.

---

13 Office for National Statistics, *Focus on the Digital Age* (2007 edition), p 2

14 Office for National Statistics, *Focus on the Digital Age* (2007 edition), pp 2, 4; Office for National Statistics, *National Statistics online*. Available at: http://www.statistics.gov.uk/CCI/nugget.asp?ID=8

15 William H. Dutton and Ellen J. Helsper, *the Internet in Britain 2007*, Oxford Internet Institute, July 2007, p 10

16 Cabinet Office, *Transformational Government: Enabled by Technology*, Cm 6683, November 2005, p 3. The emphasis appears in the original.

17 Ev 217, 222

28. Under powers granted by the Children Act 2004 and as part of the Every Child Matters Programme the Department for Children, Schools and Families is to establish ContactPoint, a database which will contain—amongst other details—minimal identifying information for every child in England, along with contact details for parents or carers, educational setting and GP practice and for other practitioners or services working with them.[18] We discuss the collection of children's data in more detail below at paragraph 92.

29. The Home Office has overall responsibility for implementing the National Identity Scheme, under the Identity Cards Act 2006. The National Identity Register will hold identity-related information, including biometric information, for everyone who has enrolled in the Scheme.[19] Anyone over the age of 16 and resident in the UK for more than three months will be eligible for an identity card. From 2011–12 the Identity and Passport Service will enrol British citizens in the National Identity Scheme "at high volumes" offering a choice of receiving a separate identity card, passport or both.[20] We discuss the National Identity Scheme in more detail below at paragraph 227.

Video or 'CCTV' surveillance

30. The Royal Academy of Engineering argues that the extent of recent technological developments in video surveillance, such as the capacity to record, store and share through digital technology, has:

> rendered tape-recorded surveillance an obsolete technology, and the term CCTV is for the most part a misleading label. Modern surveillance systems are no longer 'closed-circuit', and increasing numbers of surveillance systems use networked, digital cameras rather than CCTV.[21]

31. The Surveillance Studies Network traces the growth in use of closed-circuit television (CCTV) in the UK to the late 1980s, "prompted by attempts to reverse the decline of city centre shopping districts as well as fear of terrorism, crime and hooliganism". The Network quotes estimates that there may now be 4.2 million CCTV cameras in Britain, although the reliability of this figure is open to question, and that a person can be captured on over 300 cameras each day.[22] The Royal Academy of Engineering states that "The UK has more surveillance cameras than any other country and the number of cameras in public spaces continues to grow".[23]

32. The Home Office does not collect figures for the number of CCTV cameras. In answer to a Parliamentary Question, the Home Office said that "given the huge number of

18 HC Deb, 27 November 2007, cols 10–11WS

19 Identity and Passport Service, *About ID cards and the national identity scheme*. Available at: http://www.ips.gov.uk/identity/scheme.asp

20 Identity and Passport Service, *When will the first cards be issued?*. Available at: http://www.ips.gov.uk/identity/faqs-topten-issued.asp

21 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 33

22 Surveillance Studies Network, *A Report on the Surveillance Society: Public Discussion Document* (September 2006), pp 7–8; Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new postscript* (March 2007), p 19; ACPO queries this total: see Qq447–48 and Ev 94

23 Ev 166

cameras, operated by a very wide range of individuals, private organisations and public bodies, it is very difficult to accurately assess the total number employed".[24]

Awareness of surveillance and surveillance-related concerns

33. The publication of the report by the Surveillance Studies Network generated a great deal of coverage in the media and prompted headlines about "Big Brother Britain".[25] Several individuals who submitted evidence to our inquiry set out their concerns about living in what they saw as a surveillance society. One associated the introduction of identity cards with "the drift of the state towards surveillance" and the alteration of the relationship between the state and the citizen:

> Personally, I don't mind the state knowing where I am, but I do object to the state having the right to know.[26]

34. A survey conducted by the Information Commissioner's Office in 2005–06 found high levels of concern amongst individuals about the use, transfer and security of their personal information. In 2005–06 the survey found that 80% of individuals held such concerns.[27] In another survey, conducted in February 2008, after the HMRC incident and other high-profile data losses from public bodies, 85% of respondents said that they worried more about the safety of their personal details than they used to and 72% said that they felt powerless over how their personal information was looked after.[28]

35. The Information Commissioner told us, however, that his work on surveillance had been designed as a "wake-up call" and that there was a "need for the public to be aware of what is going on".[29] In particular the Commissioner pointed to a lack of awareness that advances in technology have had a significant impact on the extent to which everyday activities may be subject to surveillance.[30]

36. **Advances in technology have supported a significant increase in the potential for surveillance of the activities of individuals in the United Kingdom. We welcome the Information Commissioner's efforts to raise awareness of this trend, particularly in relation to the collection of personal data, and to encourage the Government to consider the implications of the growth of surveillance for the individual and society. We recommend that the Information Commissioner lay before Parliament an annual report on surveillance, and that the Government produce a response to each report, also to be laid before Parliament. We further recommend that Parliament have the opportunity to hold an annual debate on this issue.**

24 HC Deb, 8 January 2007, col 128W

25 e.g. "How we may all be microchipped like dogs in Big Brother Britain", *Daily Mail*, 30 October 2006

26 Ev 112

27 Information Commissioner's Office, *Annual Report Summary 2005–06* (July 2006), p 13

28 Personal Information Survey, prepared on behalf of Tri Media by ICM Research for the Information Commissioner's Office. Available at: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

29 Q 1 (Richard Thomas)

30 Ev 196

3 Why has the use of surveillance increased?

Introduction

37. In considering the growth of databases and forms of surveillance, we set out to identify the factors and trends which have contributed to this growth. Technological developments have increased capacity for surveillance, particularly in terms of the storage of large volumes of data, and the ability to search databases and share information through the use of interoperable systems. The commercial sector has sought to harness this new capability, recognising the competitive advantage that information about customers can bring when used to focus marketing and to design services. In the public sector this kind of technology is also used to facilitate the administration of services and in relation to matters such as border control and crime.

38. We begin by outlining the most significant technological developments in relation to surveillance potential. We move on to consider what motivates businesses to exploit this potential and how the private sector regards personal information as a valuable commodity. We then explore some of the Government's recent initiatives to collect and share information in a more efficient way, in order to deliver personalised, convenient services to citizens. We look at the public's expectation that Government agencies should provide services in a way which mirrors the techniques of the private sector, and we conclude by considering explicit calls for public bodies to collect and share more information about individuals and their activities.

Technological developments

39. Annexed to this report is a more detailed summary of the evidence and other material we considered on technological developments in relation to surveillance.

Databases and profiling

40. An increase in the storage capability of databases has been accompanied by the development of sophisticated technologies with the capacity to match and analyse different data-sets to reveal patterns. Where databases contain personal information, these kinds of technologies may be used to create profiles which in turn are produced "to make predictions about people and their likely behaviour … [that] can be used in marketing, insurance, the health service and the financial sector".[31] The Surveillance Studies Network adds to this list the development of "smart borders" and the use of passenger information to create "watch lists" of "dangerous passengers" or "identity groups" which might be regarded as posing a greater risk than others.[32]

31 Ev 166

32 Surveillance Studies Network, *A Report on the Surveillance Society: Public Discussion Document* (September 2006), p 6

Profiling

Databases may be searched automatically or 'mined' using a formula or algorithm—which may itself have been created automatically by a computer program—in order to identify and classify individuals into categories or groups on the basis of their recorded preferences or activities.

Search engines

41. Ross Anderson, Professor of Security Engineering at the University of Cambridge and Chair of the Foundation for Information Policy Research, Pete Bramhall, Manager, Privacy and Identity Research, Hewlett-Packard Laboratories, and Dr Andy Phippen, Lecturer at the School of Computing, Communications and Electronics, University of Plymouth, agreed that in terms of surveillance capacity, the most significant technological development of the last 10 years had been the search engine. Professor Anderson said:

> Previously, lots of information about people was kept on numerous, disparate databases, and a lot on paper in filing cabinets. Search engines mean that everything that is searchable is now findable if people have got the wit to look for it, and of course there are not merely the publicly available search engines, such as Google; there are search engines available to government and intelligence services which give access to information which is not generally available to the public. But overall the killer technology is search engines.[33]

42. Pete Bramhall told us that, "coupled with search engine technology", he would add "the fairly recent rise in social networking capabilities on the Internet, the rise of things like MySpace and YouTube where people can post information about themselves".[34] The Information Commissioner told us that "the growth of social network sites and online blogs raises the prospect of individuals leaving themselves open to increased surveillance".[35]

Commercial motives for exploiting surveillance potential

The force behind technological change

43. We heard our witnesses compare the various factors that contribute to technological change in relation to surveillance. Professor Anderson told us that:

> The UK is rather odd in that over the last few years a majority of the business won by our big systems houses has been public sector business rather than private sector

33 Q 180 (Professor Anderson)

34 Q 181 (Pete Bramhall)

35 Ev 259

> business, but they are almost never developing new technology, they are simply using technology which has been developed mostly elsewhere for private-sector purposes.[36]

44. Mr Bramhall and Dr Phippen added that take-up of new technologies, and attitudes towards them, could also drive technological development in making it a commercial success. Mr Bramhall said that "perhaps one of the drivers is actually coming from … the recognition by the young that technology is definitely not to be feared".[37] Dr Phippen told us that from his perspective—research into public attitudes towards and engagement with ICT—more unpredictable than technological developments themselves was the way in which those developments were used:

> I think there is an awful lot of, if you like, accidental adoption that goes on where people do things in a way that perhaps the creator of the technology did not think … it is really the use and abuse of the technology in unpredictable ways that is the difficult thing to foresee.[38]

The personalisation of products and services in the private sector

45. Commercial organisations collect and store personal information to target their communications and tailor their services. Nick Eland, Tesco's Legal Services Manager, told us that Tesco's Clubcard scheme offered benefits to customers but that:

> to offer them we need a certain amount of information to ensure that the way we communicate with them and market to them fits what they want to hear and see … We collect all their data and create profiles about those customers, better to understand their behaviour, again to ensure that when we do contact them we do so for the right purposes and in relation to products that would be of interest to them.[39]

46. Tesco employs the company Dunnhumby to analyse the data from its cards. Nick Eland, Head of Legal Services at Tesco, emphasised that the aim of analysing the information was to provide products which matched consumers' needs more closely, and that Tesco's interest in the activities of individuals themselves was limited:

> Dunnhumby does a lot of analysis on anonymised data; it is not looking at individuals but trying to look at broad ranges of customers as a whole better to understand their behaviour and enable us to achieve the goal of the scheme.[40]

47. Lenders use the information collated by credit reference agencies to make decisions on loan applications. Mike Bradford, Director of Regulatory and Consumer Affairs at Experian, a credit reference agency, told us that "the consumer will be looking for speedy access to goods and services at a competitive rate and equally a lender needs to make a responsible lending decision".[41]

---

36 Q 184 (Professor Anderson)

37 Q 185 (Pete Bramhall)

38 Qq 190–1 (Dr Phippen)

39 Qq 122–3 (Nick Eland)

40 Q 138 (Nick Eland)

41 Q 113 (Mike Bradford)

48. Stephen Sklaroff described the change that technology had made to the context for credit-related decisions:

> this technology and the existence of CRAs [credit reference agencies] has come about because the credit market now is very different from what it was perhaps 30 years ago. Then one's only way of getting credit in the legitimate regulated market, to put it that way, was to go to the local bank manager who would bring to bear to his decision whether or not to lend any personal knowledge he might have about the applicant or his family … There are huge advantages to the consumer in the situation we now have where it is not reliant on that kind of immediate personal knowledge; it is a little more anonymous. But in order to make that system work one has to have reliable data on which the lender can draw in order to make a decision.[42]

49. Companies which run search engines, collect and retain information that can link specific searches to individual users—search terms, Internet Protocol or IP addresses (an IP address is the unique identifier of a computer connected to the internet), and details of how searches have been performed—in order to improve the way in which a search engine returns results in response to users' searches.

50. The company Phorm has designed Webwise and OIX, services which track internet users' online behaviour in order to increase the effectiveness of advertising on the internet. These services have been taken up by some of the UK's biggest internet service providers but have been criticised on the grounds that if they are activated without the consent of the user, they infringe privacy and may fall foul of laws regulating the interception of communications.[43] Phorm has given assurances that:

> the systems have been configured so that the company does not have a record of the actual sites visited and search terms used by the user and in addition the advertising categories exclude certain sensitive terms and have been drawn widely so that the profiles that they hold for users will not inadvertently reveal the identity of a user or return advertising of a sensitive nature … the ISP does not hold or have access to either the advertising categories users have been matched against or the user ID and does not keep a lasting record of internet traffic for any reason other than it would have originally.

51. In April 2008 the Information Commissioner took the view that Phorm could operate Webwise and Open Internet Exchange (OIX) in a way which is in compliance with the Data Protection Act and Privacy and Electronic Communications Regulations but must be sensitive to the concerns of users.[44]

52. **Technological advances in terms of the collection, storage and use of personal information have enabled the private sector to target its communications at particular groups of consumers and to provide more personalised services. The development of this capability has produced an increasing reliance on digitally-supported means of**

42 Q 115 (Stephen Sklaroff)

43 "Phorm's internet-tracking service is 'illegal'", *Times Online*, 18 March 2008

44 Information Commissioner's Office, *Phorm—Webwise and Open Internet Exchange: The Information Commissioner's current view on the Phorm Webwise and Open Internet Exchange products*, April 2008. Available at: http://www.ico.gov.uk/

making decisions. We do not dispute the benefits to the consumer of an impartial decision-making process on the one hand and a more appropriate and convenient service on the other. We do, however, note that these benefits depend on the accuracy of the data collected and the security of the systems in which the data is held.

The value of information: profiting from surveillance

53. The Information Commissioner told us that "vast amounts of information are held on each of us in the private sector, in the financial area, in the retail area, loyalty cards and the credit reference agencies".[45] The value of information on people's commercial activities—their buying preferences, shopping habits and consumer routines—has long been recognised by the private sector as a source of competitive advantage.

54. Tesco introduced its Clubcard scheme in 1995. Mike Tattersall, retail analyst at Cazenove, said in 2006 that Clubcard has since played a key role in Tesco's expansion, conveying "an array of material benefits across virtually every discipline of its business", and constituting "Tesco's most potent weapon in the ongoing battle for market share".[46] Dunnhumby makes about £30 million a year by selling Tesco data to more than 200 consumer-goods companies,[47] and has recently agreed to an extension of its work for Tesco into nine new markets worldwide.[48]

55. Despite the potential for profit and the technological capacity to cross-reference information collected for different purposes, witnesses representing private sector organisations told us that there were limits to the ways in which companies would use personal information. For example, whilst Tesco offers personal finance services such as insurance, Nick Eland told us that information collected in applications "would not" be cross-referenced with buying patterns:

> The scheme relies on customers trusting us and valuing the scheme. In our view, those kinds of actions would massively reduce that trust and, therefore, would not make the scheme effective. It is there to reward our customers primarily, and therefore, the concept of that sort of exercise would just damage the trust of the customers that shop in our stores.[49]

Privacy gains: profiting from protection

56. The association between the collection of information and the trust of the public is one which links the surveillance carried out in the private and public sectors. We returned to this issue on a great many occasions during our inquiry. In the case of the private sector, several of our witnesses saw a direct link between trust and profit, which created a commercial imperative to protect personal information and privacy: losing the trust of customers would result in loss of revenue. The Information Commissioner told us that "in

45 Q 10 (Richard Thomas)

46 "Eyes in the Till", *Financial Times*, 11 November 2006

47 *Ibid.*

48 "Dunnhumby and Tesco team up to benefit consumers around world", Tesco press release, 14 April 2008

49 Q 133 (Nick Eland)

the private sector there are pressures to get it right which do not necessarily exist in the public sector".[50]

57. We put the Commissioner's assertion to LMG, which runs the Nectar scheme. Martin Briggs, LMG's Corporate Affairs Director, told us that:

> Data is our business; it is what we do. It is absolutely fundamental to getting it right that the trust of the collector is enhanced … We are a commercial organisation and if we do not get it right we do not make money.[51]

Political impetus for surveillance in the public sector

Harnessing technology and sharing information

Transformational Government

58. The *Transformational Government* strategy, published by the Cabinet Office in 2005, set out a vision for the better use of technology to deliver public services and policy outcomes that have an impact on citizens' daily lives:

> through greater choice and personalisation, delivering better public services, such as health, education and pensions, benefiting communities by reducing burdens on front line staff and giving them the tools to help break cycles of crime and deprivation; and improving the economy through better regulation and leaner government.[52]

Better use of technology in Government has involved a determination to facilitate greater sharing of information across departments.

59. Two of the strands of work forming part of the Strategy are Shared Services and Common Infrastructure. John Suffolk, Her Majesty's Government Chief Information Officer outlined the aim behind these strands:

> To enable greater certainty over the quality of the computer systems and networks that store and process Citizen Data it is logical to reduce these to a smaller number and share them so that greater investment and protection can be applied to the few rather than spread over the many.[53]

50 Q 10 (Richard Thomas)

51 Q 144 (Martin Briggs)

52 Cabinet Office, *Transformational Government: enabled by technology*, Cm 6683, November 2005, p 3

53 Ev 254

Government Chief Information Officer

Her Majesty's Government Chief Information Officer chairs the Chief Information Officer Council (CIO) Council, which brings together CIOs from across all parts of the public sector.

According to the Government CIO, his role is to work with departmental CIOs and those undertaking IT-enabled change to ensure that their work is aligned in supporting the Transformational Government Strategy. The Government CIO provides leadership to the IT profession across the wider public sector, enables public service transformation through the strategic deployment of technology, drives the development of shared services and acts as the 'face' of UK Government IT at home and abroad.[54]

We refer to the work of the CIO Council below at paragraph 137.

Information-sharing: improving public services by gaining public trust

60. In September 2006 the Government published its *Information sharing vision statement*. This set out the Government's aim to:

> ensure that information will be shared to expand opportunities for the most disadvantaged, fight crime and provide better services for citizens and business, and in other instances where it is in the public interest.[55]

The statement said that work to develop an identity management framework in the public sector would reduce the number of occasions on which individuals were incorrectly identified, and so given the wrong advice or directed to the wrong services.[56]

61. The statement also committed the Government to exploring how it might "provide citizens with more information about which public sector bodies hold information and what they use it for", a step which would act:

> both to reassure citizens and to support public service effectiveness in enabling people to play their part in ensuring that information held about them is accurate and up-to-date.[57]

Service transformation

62. In December 2006 HM Treasury published Sir David Varney's report on *Service Transformation: a Better Service for Citizens and Businesses, a Better Deal for Taxpayers*. In the foreword to his report Sir David said that:

54 Ev 253

55 *Information sharing vision statement*, September 2006, pp 3–5

56 *Ibid.*, paras 13 and 16

57 *Ibid.*

> Technology has enabled a revolution in the way service providers interact with their customers. These changes are continuing as citizens and businesses seek better value for money and greater convenience.[58]

63. Sir David argued that service transformation was "not about … investing in new technology" but rather that it was concerned with co-ordinating services "more directly around the needs of citizens and businesses" by means of measures such as "improved co-ordination of front-line e-services" and "reducing duplication of business processes through shared use of an identity management system". Amongst the changes recommended by the report were those which promoted the use of electronic means of entering, storing and sharing information in order to provide services".[59]

64. A report on the Government's policy review of public services, carried out in 2006 and 2007, made several references to the benefits of sharing data across Government and to the Government's desire to harness all available technology in delivering public services:

> Sharing data between health and education services might help to provide a more comprehensive response to citizens' need than if these services were to act independently.[60]

> It is now theoretically possible to compile a comprehensive DNA database and to use biometric identification on an identity card or an electronic patient record. The combination of these databases could be very effective in delivering personalised healthcare services—as well as in other areas, such as combating crime.[61]

65. One of the most widely publicised conclusions of the Review team echoed Sir David Varney's conclusion that it was difficult for public services to be responsive to demand because of rules on data-sharing. The experience of a family who had a total of 44 contacts with government over 180 days in an effort to make necessary arrangements after a member of the family died in a road accident, was given as an example of such difficulties.[62]

66. The Review report stated that "the public must be confident that the information gathered will not fall into the wrong hands and be misused" and that "the Government recognises the importance of ensuring that data and information sharing are done responsibly".[63] In response to the findings of the Review, however, the Information Commissioner's comments registered a degree of concern at the Government's drive to collect and share information:

> There are reasons why we need to promote better information but whether the right answer is to create a database should be questioned.[64]

---

58 Sir David Varney, *Service Transformation: a Better Service For Citizens and Businesses, a Better Deal for Taxpayers*, December 2006, p 1

59 *Ibid.*, pp 2–3

60 Prime Minister's Strategy Unit, *Building on Progress: Public Services* (March 2007), p 19

61 *Ibid.*, p 20

62 "Whitehall plan for huge database", *BBC News Online*, 21 March 2007

63 Prime Minister's Strategy Unit, *Building on Progress: Public Services* (March 2007), p 20

64 "Whitehall plan for huge database", *BBC News Online*, 21 March 2007

Meeting public expectations generated by technological developments and private sector services

67. We asked the Government's Chief Information Officer for his assessment of the most significant developments in technology from the point of view of delivering public services. John Suffolk identified three key developments:

- Growth of the Internet: underpinning most major economies and most successful businesses
- Convergence of communications methods: blurring boundaries between mobile communications and fixed lines
- Decrease in the size of devices.[65]

68. The combined effect of these developments has been significant in terms of Government's use of technology to collect, store and search personal information. John Suffolk told us that Government had to harness new capability in order to meet expectations that public services should be delivered in the same convenient way as private sector services are provided:

> When you put those things together what is happening is that every technology and every system is available where you are when you want to use it and that fundamentally is changing citizens' outlooks and customers' outlooks in terms of what they see as the normal service that they expect. It is not a service for our convenience; it is a service for their convenience, and those things are happening in every walk of life.[66]

The move towards personalised public services, accessed in ways which meet the needs and wishes of the individual, reflects trends observed in the private sector and has led to the collection and storage of increasing amounts of information.

Public demand for surveillance

69. The public may have come to expect from government the ability to handle information and deliver personalised services in the same way as the private sector, and may not necessarily see the collection of information for the delivery of these services as surveillance. In other areas, increases in the reach and extent of surveillance have been implemented amidst explicit calls for such increases from some sections of the public.

70. When we asked the Information Commissioner about the social impetus for surveillance he identified "one of the dilemmas" faced by his Office:

65 Q 398 (John Suffolk)

66 *Ibid.*

> by and large people value their own privacy very significantly indeed. They want their own personal information safeguarded to a great extent … They are rather less concerned about other people's privacy and other people's data.[67]

Surveillance cameras

71. We explored with the Information Commissioner two areas in which we had detected that there was public demand for surveillance and information-sharing for the purposes of public safety: CCTV or surveillance camera coverage and the sharing of intelligence held by the police.

72. The Commissioner told us that he fully accepted that "there is and has been for some time strong demand for CCTV".[68] Several Home Office studies have found evidence of strong public support for surveillance cameras. One found that "the level of support for CCTV remained high at over 70% of the sample in all but one area" of the 13 schemes the study had assessed.[69] Other research found that "levels of support for CCTV are high, although it was not clear that respondents were fully informed about how it functioned".[70]

The Bichard Inquiry and the sharing of police intelligence

73. The Bichard Inquiry into the events surrounding the Soham murders in August 2002 made recommendations for a new system to enable not only information about convictions but also police intelligence to be made available for the purposes of public protection. Whilst David Smith, Deputy Information Commissioner, rejected allegations made at the time of the Inquiry that data protection legislation was to blame for information about Ian Huntley not being shared, he acknowledged that "there was pressure for more sharing of information".[71]

74. The Deputy Commissioner told us that "it was not a question of more information needing to be made available; the system that was there did not work". He went on to say that there was "much to be commended" about the system that is now in place but suggested that the implementation of the new system had significant implications for individual privacy:

> we remain convinced that we could have had a system that protects children just as well with less impact on individuals' privacy; without things like shoplifting convictions that people had when they were teenagers coming out 15 years later when they apply for a job. It is a complex problem, and the solution is not sophisticated enough. We could have done better.[72]

---

67 Q 6 (Richard Thomas)

68 *Ibid.*

69 Gill and Spriggs, *Assessing the impact of CCTV* (London: Home Office Research, Developments and Statistics Directorate, 2005), p ix

70 Spriggs, Argomaniz et al, *Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV"*, Home Office Online Report (October 2006), p 49

71 Q 7 (David Smith)

72 Q 9 (David Smith)

75. In setting out the steps taken by the police to implement standards in relation to data security and information-sharing, Chief Constable Peter Neyroud, Chief Executive of the National Policing Improvement Agency told us that the police were "about three-quarters of the way down the list of Bichard's recommendations" and that the establishment of the Police National Database (a single source of detailed information relating to people, objects (such as cars), locations and events that will link data currently held on local systems with that held on national systems such as the Police National Computer (PNC)) would signal the completion of "the major recommendations under Bichard".[73]

Conclusion

76. **A strong common theme is emerging in both the private and public sector: a move towards more personalised services which require the service provider to collect information from individuals in order for the service to be effective. Whilst the outcome may be more personalised, however, the trend in terms of input is a standardisation of the information requested with a tendency to collect information which may identify an individual even where this is not needed in order to provide or improve services.**

77. **We recognise the desire of private and public sector service providers to make full use of the opportunities provided by technology in relation to targeting and facilitating access to services and products. We also accept that advances in technology have heightened the public's expectations of what technology can deliver not only in terms of convenience but also in connection with the prevention and investigation of crime. The elimination of technological barriers to the collection, storage and sharing of large volumes of information, however, has significant implications for individual privacy and potentially for society at large.**

78. **The Government should be open about its intentions in relation to collecting personal information, and should make sufficient time for public and Parliamentary debate on its proposals. In general the Government should move to curb the drive to collect more personal information and establish larger databases.**

73 Q 468 (Chief Constable Neyroud)

4 What are the implications of the growth in surveillance for the individual and society?

Introduction

79. In considering the factors which have contributed to a growth in the use of databases and other, more readily-recognised forms of surveillance, we have observed a tendency toward extremes in the arguments over the issues involved and the term itself. The suggestion that technology—cameras, databases of personal information including biometrics and DNA—can prevent or solve crime, secure our borders and verify our identities, stands in stark contrast to warnings about Big Brother Britain.

80. The Surveillance Studies Network acknowledges that the phrase 'surveillance society' has connotations which might promote such a polarisation of views, noting that "conventionally, to speak of surveillance society is to invoke something sinister, smacking of dictators and totalitarianism." The Network argues that the surveillance society is "better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy".[74]

81. The Information Commissioner told us at the outset of our inquiry that "this is not a one-sided debate; this is a debate about balance and where lines should be drawn." He went on to say that there were "very clear benefits" in the use of surveillance:

> We are very clear … that each individual initiative may have very well intentioned benefits in terms of the security and the safety of the public; and in terms of improvements to public and private services providing quicker, cheaper and a wider range of benefits to the public.[75]

The Commissioner also said that "it is important to recognise that there can be risks … to individuals … and there can be risks to the fabric of society as a whole".[76]

82. Throughout our inquiry we asked our witnesses and other interlocutors how they weighed up the benefits to be gained from surveillance, against the potential practical risks to the individual and the cumulative risks to society of a trend towards the collection of more information about our daily lives. We discuss those benefits and risks which are directly associated with the work of the Home Office and the fight against crime below at paragraph 198.

74 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March 2007), p 1

75 Q 1 (Richard Thomas)

76 *Ibid.*

Benefits of surveillance

Benefits to the consumer

83. We discuss above at paragraph 53 the commercial impetus to collect and store information about consumer behaviour. In using the information in order to provide more personalised services and more cost-effective marketing, commercial organisations attract more business from customers such as those who sign up to loyalty programmes, collect 'points' in return for their purchases and receive rewards, often in the form of vouchers for products or services.

84. We heard from the Finance & Leasing Association (FLA) that the use of information collated by credit reference agencies benefits the consumer in enabling lenders to:

> intervene with consumers and talk to them if it appears that the consumers are … at the tipping point … in a situation where they have what appears to be a manageable amount of debt but may be trying to contract for too much which will take them into a situation of over-indebtedness. There are things that the lender can then do.[77]

Stephen Sklaroff of the FLA also told us that technology and the development of credit reference agencies had changed a situation in which lending decisions were made on the basis of the "immediate personal knowledge" a local bank manager had of a prospective customer and that this afforded "huge advantages to the consumer".[78]

85. Martin Briggs, Corporate Affairs Director, told us that the Loyalty Management Group collected consumer data "basically to be able to track people's shopping behaviour and to be able to market offers that they will find acceptable".[79] We asked Tesco about offers on high-fat, high-salt or alcohol products in the context of responsible lending and selling. Nick Eland, Legal Services Manager, told us that customers who bought a lot of wine might receive a wine coupon but that Tesco would never promote "tobacco or baby formula or those kinds of areas". He said that "ultimately we have to rely on our customers to make the decision in relation to the information and the offers provided to them".[80]

Benefits to the patient and public health

86. Data collected about individual patients for the purposes of administering care may have a valuable secondary use in the context of medical research and the introduction of electronic patient records has provided further scope for such research. In 2006 the Academy of Medical Sciences produced a report on *Personal data for public good: using health information in medical research*. The report concluded that:

77 Q 114 (Stephen Sklaroff)

78 Q 115 (Stephen Sklaroff)

79 Q 128 (Martin Briggs)

80 Qq 140–1

> The United Kingdom already has an outstanding record in this area of research. We now have the potential to become a world leader through the opportunities offered by the NHS and new initiatives to develop national electronic care records.[81]

87. Professor Carol Dezateux of the Institute of Child Health at University College, London, appearing on behalf of the Academy of Medical Sciences, listed five kinds of research which are assisted by the use of patient data:

- Identification of the causes of disease (significant in terms of public health and finding treatments)
- Identification of effective treatment (and the potential adverse effects of treatments)
- Monitoring of public health (in terms of control of infections and epidemics) and the effectiveness of any interventions to control outbreaks
- Protection of patients and the public (in terms of safety of medicines, vaccines or in relation to environmental issues)
- Evaluation of health services (including comparative assessments).[82]

88. Professor Dezateux told us that the link between smoking and lung cancer, observed by Sir Richard Doll, was established by the secondary use of patient data and that this kind of data continued to form an important part of work to improve public health:

> As we have gone through the whole tobacco control process, it has been informed at every stage by this kind of data, and now we are looking to using this kind of data to see whether we are getting the correct response and results to this kind of intervention, and whether there are any sectors of society that are being excluded or who are continuing, for example children, to be exposed and where perhaps we need different measures.[83]

89. Professor Dezateux argued that the introduction of the NHS electronic patient record as part of a system in which records could be linked by a single identifier, would bring about a "huge advance" in this kind of research:

> One of the things it allows us to do is to be inclusive in our research so that we do not leave certain sections of the population out. It can help us get swift answers. It helps us look at areas of medicine that we are often criticised for not spending enough time on in our research: rare disorders, under-served populations. It helps us look at demographic change in a dynamic way … what happens to mothers/parents and their children and subsequent generations.[84]

81 Academy of Medical Sciences, *Personal data for public good: using health information in medical research*, January 2006, p 3

82 Q 237 (Professor Dezateux)

83 Q 238 (Professor Dezateux)

84 Q 250 (Professor Dezateux)

90. The Department of Health told us that holding care records on a national database would "deliver very significant benefits for safety and the efficient management of NHS services, improving healthcare outcomes for millions whilst preventing thousands of unnecessary deaths".[85]

Benefits to the citizen and society

91. The Government's *Information sharing vision statement*, published in September 2006, set out how information-sharing between public sector organisations and service providers had been used to deliver better public services at national and local levels, for example through:

- provision of simple-to-use electronic alternatives to postal and face-to-face services such as the Driver and Vehicle Licensing Agency's re-licensing and off-road notification service for individual vehicles over the telephone and internet which links databases holding information about vehicle insurance and MOT certification with DVLA's register of vehicles.

- reduction of the regulatory burden on business through the International Trade Single Window Project—the outcome of joint work by HM Revenue and Customs (HMRC), the Department for Business, Enterprise and Regulatory Reform, the Department for the Environment, Food and Rural Affairs, and the Food Standards Agency, which aims to allow UK businesses to provide standardised information once and then share the information with the main departments involved in authorising exports and imports.

- more efficient and effective implementation of policy through targeted efforts based on information-sharing by HMRC and the Department for Work and Pensions, which enabled the Government to identify from income and capital information people who might be entitled to claim Pension Credit but who were not doing so.[86]

92. The Department for Children, Schools and Families told us that much of its activity depended on effective information-sharing "both at the level of Government databases, and between individual practitioners", and that this work was "central" to the Department's ability to "deliver better outcomes for children and learners". The Department listed several kinds of benefits to be gained from sharing information:

> Better information sharing is crucial to safeguarding children and supporting the drive to personalise learning and to improve service delivery; it also contributes to improvements in efficiency and effectiveness, in reducing burdens on the front line, and in ensuring effective accountability. It [information-sharing] is a cornerstone of the Every Child Matters (ECM) strategy to improve outcomes for all children and for delivery of many of our reform programmes such as specialised diplomas and vocational qualifications reform.[87]

85 Ev 218

86 HM Government, *Information sharing vision statement* (September 2006), pp 3–4

87 Ev 245

Weighing up the benefits of surveillance

93. In examining the potential gains to be made from surveillance—from the point of view of the individual and of society as a whole—we heard a range of views from those who sought to explore how these gains might be measured against the cost in terms of resources and the impact of intensifying surveillance on our daily lives. The main arguments we heard against ready acceptance of surveillance as a social good were that the benefits of surveillance should be seen in the context of the amount of personal information given up by the individual—questioning whether or not the same benefit could be achieved without some of this information—and that resources devoted to surveillance could be better deployed in other areas. We discuss the use of surveillance cameras in this context below at paragraph 201.

94. Having commissioned research on the use of databases of information about children, the Information Commissioner's Office told us that gathering more and more information about individuals could hinder rather than help Government in achieving its aims, particularly when those aims were not tightly defined. Assistant Information Commissioner Jonathan Bamford said that whilst some of its concerns about the index of all children in England, now known as ContactPoint, had been allayed as the database had been developed, the "philosophy" of the Information Commissioner's Office remained the same:

> We want information of the right quality relating to the right people who really need care and concern … where people should take seriously the responsibilities in respect of those children. The simple acquisition of more and more information does not actually mean that people make better judgments. They will become overloaded. We have certainly heard it said from those who are involved in the early child welfare issues that sometimes it is more social workers that we need rather than more information because we already have that much information we cannot act on.[88]

95. The Information Commissioner himself underlined the need to take into account the stated aim and scope of a particular database when evaluating its benefits:

> the case for an index of children is very much greater for those children who are, or who are perceived to be, at risk, than is the case for a universal database of every child in the country in the more nebulous name of promoting their social and educational welfare. I think the second part is a great deal more doubtful.[89]

Risks of surveillance

Practical effects of misuse or mistakes

96. At the beginning of our inquiry the Information Commissioner outlined the risks to the individual which may be associated with "excessive" surveillance whether by means of cameras or other monitoring techniques such as the collection of information on

88 Q 35 (Jonathan Bamford)

89 Q 35 (Richard Thomas)

databases. For individuals, the Commissioner told us, the risk is that they will suffer harm because information about them is:

- inaccurate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- disclosed to those who ought not to have it
- used in unacceptable or unexpected ways beyond their control, or
- not kept securely.[90]

97. Expanding on this the Commissioner said that:

> The practical risks are … in terms of the detriment to individuals which can occur when mistakes are made, for example mistaken identity; where there is false matching and the wrong individual is identified; where there is inaccurate or out-of-date information; where there are breaches of security.[91]

The consequences of a black market in personal information

98. In two reports to Parliament, *What Price Privacy?* and *What price privacy now?*, published in May and December 2006, the Information Commissioner set out to expose and tackle what he described as "the unlawful trade in confidential personal information".[92] The Commissioner argued that as public and private sector bodies hold more and more personal information and as Government initiatives direct that such information is collected and shared centrally, the risk of security breaches by individuals engaging in this unlawful trade "inevitably" increases.[93]

99. The Commissioner told us that:

> For any member of this Committee or any member of the public here I could say what the tariff is for getting your personal information … I could say how much to get your mobile phone records; how much to find out if you have a criminal record or not; how much to get hold of your DVLA records to see who owns the car parked outside your house last night.[94]

Those willing to pay for such information include finance companies and local authorities seeking to recover debts, estranged couples with one party seeking to trace the other, and criminals seeking to perpetrate fraud or to intimidate witnesses or jury members.

90 Ev 197

91 Q 2 (Richard Thomas)

92 Information Commissioner's Office, *What Price Privacy?,* HC (2005–06) 1056 (May 2006); *What Price Privacy Now?*, HC (2006–07) 36 (December 2006)

93 *What Price Privacy Now?*, HC (2006–07) 36 (December 2006), p 4

94 Q 58 (Richard Thomas)

100. We asked the Commissioner to recount his experience of the impact of being the victim of the trade in personal information, including where such details are used for the purposes of identity fraud, also called identity theft:

> When people find their identity has been stolen there can be severe financial consequences. Even if the banks and others assume some ultimate liability there can be a horrendous amount of hassle and worry for people to sort matters out … If people find they are being impersonated their reputations can suffer. It can be in the workplace, it can be in their social environment, with their families … if people's private lives are unjustifiably intruded upon, there can be a very, very real deep sense of outrage.[95]

Identity fraud

The Royal Academy of Engineering defines identity fraud (or as it is often known, identity theft) as "the impersonation of someone else in order to obtain financial benefits (for example, by purchasing goods on-line) or to avoid penalties (for example, speeding fines incurred when using a hire car)".[96]

We discuss the concept of identity in the context of personal information below at paragraph 145.

Data loss and identity fraud

101. The International Association of Privacy Professionals (IAPP) drew a distinction between security breaches as a result of criminal activity and those occasions on which "people just lose disks or other back-up tapes".[97] During our inquiry, however, a series of high-profile incidents of data loss by Government agencies served to underline the risks associated not only with the abuse of surveillance by criminals but also with the collection and sharing of personal information for the purpose of delivering public services.

102. In terms of the amount of data lost, the incident reported to the House of Commons in a statement by the Chancellor of the Exchequer on 20 November 2007 was the most serious. Two password-protected discs containing a full copy of HM Revenue and Customs "entire data" in relation to the payment of child benefit—records for 25 million individuals and 7.25 million families—were sent to the National Audit Office by HMRC's internal post system (operated by the courier TNT). The discs failed to reach the NAO and were not recovered.

103. Banks and financial institutions were informed of affected accounts so that they could monitor them for irregular activity and evidence of fraud and the Chancellor asked Kieran

95 Q 66 (Richard Thomas)

96 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 25

97 Q 95 (Randal Gainer)

Poynter, Chair of PricewaterhouseCoopers, to investigate HMRC's security processes and procedures for data handling. The Prime Minister asked the Cabinet Secretary and security experts to ensure that all departments and agencies checked their procedures for the storage and use of data.[98]

104. After details of the data loss were made known to the public, APACS, the UK Payments Association, sought to reassure customers that "there is no evidence that the data has fallen into criminal hands nor that any fraud has been attempted as a result of this incident".[99] In February 2008, the security firm McAfee reported on a phishing attack that targeted victims of the HMRC data loss with an email offering the recipient the opportunity to claim a tax refund of £215 from the government and containing a link to a suspect website.[100]

Phishing

Phishing is a type of deception designed to steal valuable personal details, such as credit card numbers, passwords, account data, or other information, by means of fraudulent email messages or 'pop-ups' that appear to come from known websites such as those run by banks or credit card companies.

105. Whilst this data loss incident does not seem to have resulted in large-scale theft from the bank accounts of child benefit recipients, it has highlighted the potential consequences of compromising sensitive personal information in the terms described by the Information Commissioner.

Incorrect information and false matches

106. Another risk associated with surveillance is the danger that an individual will suffer harm not because he or she has been impersonated by someone else but because an organisation or individual targets him or her by mistake or makes decisions based on incorrect information. Where these decisions involve targeted marketing, harm to an individual might amount only to inconvenience or to missed opportunities to choose a more appropriate product or service—although concerns have been raised about the implications for individual privacy of new internet advertising services which collect information about users' internet searches[101]—but where financial, health or security decisions are concerned the potential for harm is much greater.

107. Dr Eric Metcalfe, Director of Human Rights Policy at JUSTICE, gave an example to illustrate the potential effect of surveillance-based decision-making on an individual's life:

98 HC Deb, 20 November 2007, cols 1101–04; HC Deb, 21 November 2007, col 1179

99 "Banking industry response to HMRC potential data compromise" APACS press release, 20 November 2007

100 "HMRC phishing attack offers fake tax refund", *Computerworld UK*, 25 February 2008; "Phishers slow to capitalise on HMRC data loss", *Computing*, 22 February 2008

101 See above at paragraph 50.

> Maybe someone is arrested. It is a case of mistaken identity, but someone makes a complaint about them being, say, a sex offender. They are acquitted or maybe charges are not even brought, and they think nothing of it until the next time they apply for a job working with children, and then they find they cannot because they have failed the child protection check because of the fact they have been arrested in relation to a sex offence means that that information has to be disclosed.[102]

Dr Metcalfe did not argue that this kind of information should not be disclosed in any circumstances but rather that in general "we do not have very much appreciation of the way in which information is transferred".[103]

Cumulative effect of misuse or mistakes: a disproportionate burden on the disadvantaged?

108. Whilst there are steps that individuals themselves can take to protect their privacy, and to gain access to the information held about them under the rights afforded by the Data Protection Act, to check that information is correct or to limit its disclosure to suit their needs, taking these steps requires individuals to exercise an informed choice in relation to surveillance. Those without the degree of awareness or the means to exercise this choice may therefore be at greater risk of suffering harm as a result of misuse or mistakes in information held about them; where no such choice is available their vulnerability may be compounded.

109. Throughout our inquiry we heard evidence of the strong link between choice and privacy. Witnesses representing private sector organisations emphasised the choice that consumers could exercise over providing information about themselves and the availability of choices such as obtaining credit reference reports. Mike Bradford of Experian told us that awareness of these choices was becoming more widespread:

> people are far more aware than they used to be of what a credit reference agency does. It is not Big Brother where data sits there and there are black lists with all the other very emotive things over which at one point there was concern. We have a strategic imperative in our business to work on consumer education and awareness.[104]

The Department of Health outlined the choices available to NHS patients in relation to the records of their care, including a range of 'opt out' decisions:

> Individuals who have concerns can choose not to have a Summary Care Record created for them. They will be advised to inform their GP of their views and to request that a note be made of their concerns and the choice they have made … They can alternatively choose to have a Summary Care Record created but not accessible to anyone but themselves. They will be able to access it anytime using a secure

102 Q 293 (Eric Metcalfe)

103 *Ibid.*

104 Q 164 (Mike Bradford)

> internet site called HealthSpace. Patients will of course be able to change their mind and request a Summary Care Record at any point.[105]

110. The Information Commissioner's Office works to raise awareness of the kinds of information which organisations collect about individuals, and of the individual's 'right to know'. Whilst the Commissioner told us that he was working with Connecting for Health (the agency responsible for delivering the electronic patient record) on the scope for tailoring people's use of patient information "more in line with their personal preferences", and that there was scope for developing such options in other particular areas, he argued that the choices available in the public sector were strictly limited:

> it is not like in the private sector where you do have a genuine choice: you can choose that holiday or that loyalty card or that bank account and you can shape your choices according to what is on offer. When you are dealing with the Health Service, the police, the taxman, by and large there is not much scope for choice.[106]

Deepening the 'digital divide': a 'privacy divide'?

111. Means of exercising choice over the personal information that is collected, stored and used often depends on access to technology. Whilst internet penetration in the UK has increased to 61%[107]—increasing at the same time the amount of personal information available for collection—and a range of applications and devices to detect and deter surveillance have been developed, a number of our witnesses acknowledged the concern that reliance on such developments could lead to what the Surveillance Studies Network described as "a society of privacy haves and have-nots".[108] The Government's Chief Information Officer, for example, said that it was "very important that we do not disenfranchise any section of the public by going down one particular route".[109] We discuss this issue in the context of privacy-enhancing technologies below at paragraph 152.

Profiling

112. Beyond internet penetration and a focus on electronic delivery of services, technological developments have allowed for information on different databases to be matched and to be 'mined' automatically to link data on individuals and create 'profiles' using algorithms to group individuals together according to their characteristics, preferences or activities (see above at paragraph 40). The Royal Academy of Engineering argued that in creating profiles, "categorisation is rarely perfect" and that this can lead to inappropriate groupings: in turn people could find themselves sorted and stigmatised as criminals or bad creditors. It went on to argue that profiling to identify people as potential

105 Ev 219

106 Q 34 (Richard Thomas)

107 Office for National Statistics, *Focus on the Digital Age* (2007 edition), pp 2, 4; Office for National Statistics, *National Statistics online*. Available at: http://www.statistics.gov.uk; Q399 (John Suffolk)

108 Ev 158

109 Q 399 (John Suffolk)

criminals "risks treating all people who fit a certain profile as potential terrorists or criminals".[110]

113. We heard evidence of the danger that profiling may accentuate existing social inequalities, with practical effects for the individuals involved, consequences for the privacy and liberty of those individuals, and wider implications for society. The Law Society's evidence made explicit its concern that profiling could have undesirable ramifications for individuals and society:

> Profiling in order to identify possible criminal activity is objectionable to the extent that it makes everyone a suspect. It is dangerous in its reliance on potentially inaccurate or out-of-context data and its use of unprovable algorithms. It tends towards a reversal of the normal burden of proof in both civil and criminal law.[111]

Impact of surveillance on privacy and individual liberty

114. When we asked Shami Chakrabarti of Liberty about the risks to the individual posed by a 'surveillance society', she emphasised that privacy was a qualified right and that there were "very good reasons", such as security or public health concerns, why the value of the right of privacy could be "lost or forgotten on occasion." She argued, however, that it was important for the "ethical, political and legal debate" to keep pace with the technological developments which provided new opportunities to interfere with privacy,[112] and that its value—as embodied by the concept of a secret ballot—should not be underestimated:

> Without this right, even in the human rights community, sometimes regarded as a bit low-level, a bit trivial—it is not torture, it is not arbitrary detention—you cannot have free elections, freedom of thought, conscience and religion, freedom of speech in some circumstances without that little bit of personal space and respect for it.[113]

115. Dr Eric Metcalfe, representing JUSTICE, argued that even if information held about an individual was not misused or misrepresented the fact of its storage and potential use was significant:

> if I write a diary and I leave it in a room and I am subsequently aware that maybe 10 people have gone through that room and had the opportunity to read my personal thoughts sitting on the desk, maybe none of them did, but already that has had an effect on my personal privacy. If you think about all your personal data as being in that diary and if you think about not merely 10 people passing through that room but, say, all the relevant agencies that have come on to the stage having access, then you have reason to be concerned, and your own sense of personal privacy, which we think has a very important value because it allows us to do so many things that we take for granted as being part of a good life, is affected as a result.[114]

110 Ev 166

111 Ev 172

112 Q 279 (Shami Chakrabarti)

113 Q 298 (Shami Chakrabarti)

114 Q 280 (Eric Metcalfe)

Effect on society as a whole: the question of trust

116. The Information Commissioner told us that the wider harm to society caused by excessive surveillance can include:

- intrusion into private life which is widely seen as unacceptable
- loss of personal autonomy or dignity
- arbitrary decision-making about individuals, or their stigmatisation or exclusion
- the growth of excessive organisational power
- a climate of fear, suspicion or lack of trust.[115]

117. These risks combine the practical effects of mistakes or misuse of data, with what might be regarded as more 'philosophical' concerns about the effect of surveillance on privacy and individual liberty. The Commissioner argued that these "more philosophical issues" about the collection and use of information were linked to the question "what sort of society are we content to live in?"[116]

Trust

In this report we use the word 'trust' predominantly to mean confidence in and reliance on the capabilities and good faith of a person or organisation.

118. Dr Metcalfe of JUSTICE saw a close relationship between an individual's enjoyment of his or her privacy and the value of privacy to wider society:

> personal liberty is ultimately part of the common good … we benefit not merely as individuals in having privacy, we benefit as a society: because people do things in their private space, in their private time, and the benefits from that flow on to society as a whole.[117]

In the same way Liberty argued that where surveillance put the privacy of an individual at risk, the broader relationship between citizen and state was also at stake:

> without really quite a significant degree of value paid to personal privacy, there would be a society where the dignity of the individual has been compromised; intimacy between people, confidence between people and trust in big institutions, whether it is the Health Service or the Government, would be lost.[118]

115 Ev 197

116 Q 2 (Richard Thomas)

117 Q 297 (Eric Metcalfe)

118 Q 278 (Shami Chakrabarti)

The Department of Health confirmed that patients' willingness to trust the National Health Service with their information was crucial to the delivery of individual patient care and to the success of secondary research:

> Without public confidence in how information about patients is managed we risk losing one of the fundamental tenets of how the NHS can operate.[119]

119. The primary purpose of collecting information from patients—to facilitate diagnosis and treatment—and the consequences of mistakes or security breaches—misdiagnosis, the release of sensitive information an individual might wish to keep private—are clear. However, in other contexts the methods and purposes of collecting and sharing personal information are less evident and a greater degree of trust is required on the part of the individual.

120. Where technological developments have removed technical and cost barriers to the collection, storing, searching and sharing of information we trust those who hold our information not only to keep it securely but also to refrain from using it for purposes other than those for which it was collected. Dr Chris Pounder, Editor of *Data Protection and Privacy Practice*, described the relationship this situation established between the individual and all those who bear responsibility for the collection and sharing of their information:

> The public has to trust that the datasharing is limited in accordance with the rules, the public have to trust that staff who do the datasharing are properly trained and follow the rules, the public have to trust that the procedures for authorising the data are properly maintained and the public have to trust that Parliament does not enact legislation that provides for function creep. All this trusting is in one direction.[120]

Dr Pounder told us that "if this trust is broken on occasions or generally, it manifests itself, not just in a way that is of detriment to the individual but of great harm to public policy as well".[121]

121. Other witnesses concurred that—particularly where surveillance is carried out not in a targeted way for a clearly defined purpose but as a matter of routine—erosion of trust could have serious consequences. The Royal Academy of Engineering argued that a policy of using surveillance to profile people in order to identify potential criminals could generate "distrust of the authorities that use such profiling methods".[122]

122. If individuals withdraw their co-operation from authority because they do not trust it, by refusing to provide information on a voluntary or consensual basis, in turn those in authority will need to carry out more surveillance in order to achieve their aims in terms of improving public services and enhancing public safety. This scenario might represent an unlikely outcome but it is one which several of the witnesses in our inquiry have envisaged

119 Q 326 (Richard Jeavons)

120 Q 282 (Chris Pounder)

121 *Ibid.*

122 Ev 166

as a realistic prospect, arrived at after incremental increases in the scale of surveillance effected without proper consideration of the risks involved.

Conclusion: a matter of balance

123. **The technological developments which facilitate the collection, storage and use of information about individuals and their activities have clear benefits for the individual as a consumer and a user of public services. If collected accurately and used properly databases of personal information can support both 'de-personalised', impartial decision-making processes and the delivery of 'personalised' services tailored to the needs of the individual.**

124. **However, the risks associated with the collection and use of personal information in databases in particular and the monitoring of individuals' behaviour in general, should not be underestimated. Mistakes or misuse of data can result in serious practical harm to individuals. Those less demonstrable risks which relate to the erosion of one's sense of privacy or individual liberty also have a practical aspect and a broad application in that they affect the way in which citizens interact with the state.**

125. **The risks associated with surveillance increase with the range and volume of information collected. The Government has a crucial role to play in maintaining the trust of the public: any evaluation of the use of surveillance must take into account the potential risk to this relationship with the public.**

126. **Technological capabilities continue to expand, increasing our means both of generating information about ourselves and of using that information for different purposes. But the drive to make the most of these capabilities should be tempered by an evaluation of the risks involved in collecting more information. Particular consideration should be given to situations in which individuals might suffer as a result of their lack of awareness or ability to take advantage of opportunities to exercise choice over how information about them is used, or to check that it is accurate.**

5 Are existing safeguards strong enough?

Regulatory safeguards

127. During our inquiry we heard evidence on the safeguards in place to protect individuals from unauthorised surveillance and from security breaches which might lead to the disclosure of their personal information. There are several key pieces of legislation which govern data-sharing and the protection of human rights with regard to personal data and privacy in the UK:

- the Data Protection Act 1998 governs the collection and exchange of personal data
- the Regulation of Investigatory Powers Act (RIPA) 2000 legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism[123]
- Article 8 of the European Convention on Human Rights sets out the right to privacy.

The Data Protection Act gives effect to the European Data Protection Directive. In April 2008 the Information Commissioner's Office announced that it would invite tenders to carry out a study of the strengths and weaknesses of EU Data Protection law, addressing "a growing feeling that the EU Directive on data protection is becoming increasingly outdated and is more bureaucratic and burdensome than it needs to be".[124]

128. A number of other EU instruments affect how personal information relating to UK citizens is shared within the EU and with third countries. We considered safeguards for data in this context in connection with our inquiry into *Justice and Home Affairs Issues at European Union Level.*[125]

129. The Ministry of Justice is responsible for the Government's domestic, European and international policy on data protection and data sharing.

130. The Information Commissioner's Office (ICO) administers the Data Protection Act 1998. Under the Act, a data controller ("a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed") has a duty to comply with a set of data protection principles in relation to all personal data in respect of which he is the controller.

123 See below at paragraph 311.

124 Information Commissioner's Office press release, "ICO invites tenders to review EU Data Protection Law", 14 April 2008

125 Home Affairs Committee, Third Report of Session 2006–07, *Justice and Home Affairs Issues at European Union Level*, HC 76

Data Protection Principles

1. Personal data shall be processed fairly and lawfully …

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

131. The Information Commissioner has power to conduct audit and inspections to ensure compliance with the Data Protection Act but this is limited by a requirement to have the consent of the data controller concerned. Where data protection principles are breached the Commissioner has the power to issue enforcement notices which are remedial in effect. The Commissioner told us that these "do not impose any element of punishment for wrong doing".[126] Offences under the Act are punishable by fine.

132. The ICO also administers the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

133. In conjunction with its two main aims—to ensure that public information is available to all, unless there are good reasons for non-disclosure and to ensure that personal information is protected—the ICO works to encourage organisations to adopt good practice in relation to handling data and information, and to influence thinking on privacy and access issues.

134. The ICO has drawn up codes of practice for the sharing of personal information and the use of CCTV and the Commissioner provides advice to public and private sector

126 Ev 199

bodies on new practices and projects which involve the collection and use of personal information.[127]

Responsibility for protecting information in the public sector

135. The Government's Chief Information Officer outlined the following "roles and accountabilities" in relation to safeguards for data held by public bodies:

Accounting officers

136. The Accounting Officer of a public sector body is accountable for ensuring that:

- personal information (or "Citizen data") is used for the purposes for which it was intended in accordance with the relevant legislation
- the appropriate policies, procedures, staff and technology are deployed to maintain standards for keeping citizen data accurate and for protecting it from disclosure
- defined roles and responsibilities within the organisation relate to the execution of risk identification and mitigation strategies for the use of citizen data

Chief Information Officer (CIO) Council

137. The CIO Council's remit is to improve public service delivery by ensuring that the "strategic use of technology and computer systems are aligned" with the overall strategy set out in the *Transformational Government Strategy* (see above at para 26). The CIO Council is charged with creating and delivering a Government-wide CIO agenda to "build capacity and capability in IT-enabled business change".

Central Sponsor for Information Assurance

138. The Central Sponsor for Information Assurance (CSIA), based in the Cabinet Office, is accountable for the development of strategy, policy and guidance relating to the protection of data. The CSIA is also responsible for the accreditation of departmental computer systems and networks and for ensuring that they conform to agreed minimum standards.[128]

Debate on the limitations of regulatory safeguards

139. The Information Commissioner told us that whilst regulation formed the basis for protection of personal information and prevention of excessive surveillance, the role of the individual in seeking to check or query the collection, storage and use of information under data protection and other legislation, was crucial:

127 Information Commissioner's Office, *Framework Code of Practice for Sharing Personal Information*; *CCTV Code of Practice: revised edition 2008*

128 Ev 253

> it is about educating and encouraging people to use their own rights as much as about what we can do as the regulator.[129]

140. In the Foreword to his Annual Report for 2006–07 the Information Commissioner argued that "self interest" on the part of those organisations which control the use of personal information was also a key safeguard against the risks associated with excessive surveillance:

> Although many of the detailed rules are too bureaucratic, the underlying principles of data protection have successfully stood the test of time. They provide a sound framework to minimise the risks and promote acceptable and beneficial handling of personal information. But legal regulation is insufficient by itself. The consequences of getting it wrong can now be seen instantly—domestically and across the globe—causing great short-term damage to political and commercial reputations and long-term damage to society. It is ministers, permanent secretaries, chairs and chief executives who must ensure their organisations guarantee safeguards and exercise the necessary self-restraint. This is simple self-interest which must come from the top.[130]

141. This "self-interest", however, conspicuously failed to prevent the "great short-term damage" to the reputations of HMRC and the other organisations involved in high-profile data loss incidents in recent months. In December 2007 the Information Commissioner told the House of Commons Justice Committee that after the loss of child benefit data, public and private sector bodies had approached his office almost "on a confessional basis" to bring to the Commissioner's attention problems they had encountered with security.[131]

Technological safeguards

Privacy-enhancing technologies

142. Technologies themselves can provide powerful controls over potential for surveillance or invasion of privacy, minimising data collection and providing intrinsic safeguards. For example, encryption of personal data as it is stored or flows across domains and other electronic boundaries can provide a degree of security, network design and software code can act to restrict surveillance, and web 'cookies' can be filtered. Such methods of limiting surveillance are known as 'Privacy-enhancing technologies' or PETs.

129 Q 79 (Richard Thomas)

130 Information Commissioner's Office, Report for 2006–07, HC (2006–07) 646, p 6

131 Justice Committee, First Report of 2007–08, *Protection of Private Data*, HC 154, p 4

Cookies

A "cookie" is a small piece of information sent by a web server to store on a web browser so it can later be read back from that browser. Cookies can contain a variety of information, including the name of the website that issued them, where on the site the user visited, and user names and passwords that have been supplied via forms.

Cookies are used for a range of purposes, including: online ordering systems (and services such as Google Checkout, which allows people to buy from stores across the web and track all their orders and delivery information in one place), website personalisation, website tracking (for example, to allow a web designer to see how people navigate a particular site), and targeted marketing.

Cookies can make using the internet and online services quicker and easier for consumers but raise privacy concerns because—whilst a great many companies have cookie policies and users can choose to stop their browsers from saving cookies—they can be stored in a user's computer without the user's knowledge or consent.[132]

143. In a Communication to the European Parliament and the Council, the European Commission set out its support for PETs. It considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. Whilst the use of PETs would be complementary to the existing legal framework and enforcement mechanisms, the Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The Commission's Communication gives the following as examples of PETs:

- Automatic anonymisation of data after a certain lapse of time: this supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected

- Encryption tools: prevent hacking when information is transmitted over the Internet or other media, and support the data controller's obligation to take appropriate measures to protect personal data against unlawful processing

- 'Cookie-cutters': block cookies placed on the user's PC that make it perform certain instructions without the user being aware of them, enhancing compliance with the principle that data must be processed fairly and lawfully, and that the data subject must be informed about the processing going on

- The 'Platform for Privacy Preferences' (P3P): allows internet users to analyse the privacy policies of websites and compare them with the users' preferences as to the

132 Source: www.cookiecentral.com

> information they wish to release, helping to ensure that data subjects' consent to processing of their data is an informed one.[133]

144. Symantec, a software company which specialises in security software and services, told us that the market offered a number of a number of technological tools:

> suitable for different environments and different user-sophistication that can afford adequate levels of security and protection for personal sensitive information. The information security industry continues to develop innovative solutions that can ensure the security and privacy of individuals' information in the evolving threat landscape.[134]

145. A conference supported by the European Commission and held in November 2007—a "series of independent forums for discussing privacy in relation to the development of new technology"—took as its theme "the need for privacy and security to be designed in to products and services at the earliest stage" and concluded that "Governments are critical enablers who will control the demand for and enforcement of PETs."[135]

Digital identities and identity management

146. According to the Royal Academy of Engineering, technologies such as encryption can be used to separate *authentication*, a process that results in a person being accepted as authorised to, or having the right to, engage in or perform some activity; and *identification*, the process that results in a person's identity being revealed. For such technologies to provide an effective safeguard for personal information, however, the Royal Academy of Engineering argued:

> privacy has to be engineered into the system at the most fundamental level, allowing anonymity or at least pseudonymity of users (the ability of users to have a different pseudonym for different services) at the level of the infrastructure.[136]

147. Hewlett-Packard Laboratories, one of the leaders of the PRIME project, a "four-year co-operation between 20 industrial and academic research institutions, that aims to advance the state of the art of privacy-enhancing technologies",[137] stated that:

> There is a variety of technical approaches to providing the individual with the means to manage his/her digital identity information to and control its release and subsequent use. These range from approaches in which all communication and interaction between digital service provider and consumer is done on the basis of anonymous credentials (i.e., no identity information is transferred) to those in which the service provider's identity management systems are designed to follow all the

133 Communication to the European Parliament and the Council (COM (2007) 228 final, 2 May 2007))

134 Ev 157

135 European Commission, *A Fine Balance: Privacy enhancing Technologies: How to create a trusted information society—summary of conference*, November 2007, pp 17–19

136 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 39

137 Ev 178

> consumer's requirements regarding his/her identity information (and thus act as his/her proxy) and are verified as actually doing so.[138]

Whilst it did not advocate "the total replacement of identity-based digital service delivery systems by those in which no identity information at all is required", Hewlett-Packard Laboratories emphasised the "benefits to be gained" if identity information demanded by a service provider "be just that required to deliver the service, and no more".[139]

148. Caspar Bowden, an expert on privacy-enhancing technologies and privacy regulation, argued in written evidence that:

> Sophisticated PETs can provide much more robust bulwarks against function-creep than policy controls alone, but it must be understood that the purpose of these technologies is expressly to minimize the disclosure of personal information to the absolute minimum required.[140]

Mr Bowden said that whilst industry and academia were able and willing to develop effective PETs and privacy systems, "there is a chronic lack of awareness and interest from both data controllers and most regulators".[141]

149. According to Mr Bowden, advanced PET techniques could be used to create authentication systems which would eliminate the need for a database of all system transactions as the basis of an 'audit trail'. Mr Bowden argued that the use of these techniques was "*mandated*" by the Human Rights Act and Article 8 of the European Convention on Human Rights and that the legality of the "blanket collection of identifiable transaction data" was questionable.[142]

Debate on the limitations of technological safeguards

The role of the individual

150. We heard from our witnesses that the effectiveness of privacy-enhancing technologies in protecting individuals from unauthorised monitoring of their online activities and theft of their personal information, depends to a great extent on individuals' awareness of the need to take steps to secure the systems they use and their ability to gain access to the new technologies.

151. Pete Bramhall, of Hewlett-Packard Laboratories, said that technology such as encryption could provide effective protection but told us that "the question then becomes how do you make that usable and accessible to the ordinary person".[143] Dr Andy Phippen, of the University of Plymouth, agreed that these were key issues, arguing that the prospect of convenient access to services and other benefits was more influential than concern about

138 *Ibid.*

139 Ev 177

140 Ev 273

141 Ev 272

142 Ev 273

143 Q 205 (Pete Bramhall)

security in guiding people's attitudes towards providing personal information by electronic means:

> The public's view of encryption is whether the little padlock is on the browser and, if the padlock is on the browser, it is safe. I think the usability issues are extremely significant if you are looking at privacy-enhancing technologies at all and, unless your average person on the street is comfortable with them, guarantees of security will be ignored in a lot of the cases … If you are buying something online and you are saving yourself 50 quid, it is very clear. There are some very successful public sector e-delivery mechanisms, such as the DVLA and tax returns, and school admissions systems for some reason are incredibly popular because they offer a sort of return in terms of convenience to individuals and they are not saying "I'm not using that" because you are not using the most up-to-date encryption mechanisms on it, but they are saying, "I'll use that because it will save me having to fill out the form on paper or it saves me having to phone someone up and do it all on the phone".[144]

152. Dr Phippen told us that his research into attitudes towards responsibility for online security found that the predominant view amongst individuals was that responsibility for making sure that systems were secure rested elsewhere:

> We did an awful lot of work with awareness and education, who is responsible, and it always comes back when you talk to citizens that it is the Government and it is that manufacturers that should be responsible.[145]

Whilst Pete Bramhall argued that garnering a reputation for protecting personal data could become a differentiator for private sector companies "particularly as far as the provision of digital services is concerned", he went on to tell us that the potential of privacy-enhancing technologies had not been realised:

> increasingly as technology, particularly privacy-enhancing technology, begins to offer possibilities for system designers to design the systems in a way that actually requires less personal information, then I think the incentive to them to do so is not actually apparent at the moment because they are sort of stuck in this habit of gathering more information because it might come in useful some day.[146]

153. A regular experiment to test the security of wireless networks carried out by Dr Phippen's students found that the number of unsecured networks had dropped significantly in the past two years. Dr Phippen attributed this change to the fact that vendors of computer equipment "are now providing out of the box some level of security". He said that whilst "manufacturers are trying to do more" in terms of building security measures in to the products they sold, another experiment showed that over 60% of people who were sent an unsolicited message on their unsecured Bluetooth devices received the message and loaded it up. Dr Phippen concluded from this experiment that although

144 Q 205 (Dr Phippen)

145 Q 197 (Dr Phippen)

146 Q 210 (Pete Bramhall)

manufacturers could "do a lot" and Government, through education, "is not doing enough" to protect privacy:

> there has to be personal responsibility because ultimately it is a personal device … people were very willing to accept that something is in their personal device, they did not know what it was, they just accepted it. Now, how could a manufacturer protect against that?[147]

PETs and a 'privacy divide'

154. The Surveillance Studies Network insisted in its evidence that PETs could not be regarded as a panacea, asking:

> Do PETs represent simply a market response to problems of surveillance and privacy? If so, their spread and relative effectiveness will replicate social and economic divisions, leading to a society of privacy haves and have-nots.[148]

The Network posits the emergence of "Personal Information Economies" where the wealthy are able to enjoy the benefits of surveillance (for example, as consumers or users of public services) and "technologically-enhanced privacy" but the "poor, marginalised and excluded" who are unable to gain access to such technologies, are simply subjects of "mass surveillance, categorisation and control".[149]

155. We put to our witnesses the concerns of the Surveillance Studies Network that reliance on privacy-enhancing technologies to protect personal information online could create a 'privacy divide' between those who could afford to invest in technologies to protect themselves from excessive or unwarranted surveillance and those who could not. In discussing a "privacy-enhanced approach", Pete Bramhall's view was that in terms of the price of privacy-enhancing technologies:

> the issue then becomes whether the providers of digital services would wish to price perhaps discriminatorily such that the privacy-sensitive services are at a higher price than the other ones. I think then perhaps it becomes a question for society as to how much it is willing to countenance the possibility of a privacy divide, as you described it.[150]

Privacy-enhancing processes: the role of the organisation

156. Professor Anderson told us that having been involved in developing a number of "what would now be called 'privacy-enhancing technologies'", he had become "something of a sceptic". He argued that "they can be dressed up in various fancy ways, but at heart they are pseudonyms" and that their value was limited because organisations could profit from collecting personal information:

147 Q 197 (Dr Phippen)

148 Ev 161

149 *Ibid.*

150 Q 206 (Pete Bramhall)

> Companies do not want to deal with pseudonymous individuals, by and large, unless there is some premium in it for them. You can get prepaid credit cards, but they are significantly more expensive and the reason for this is that the information that is collected about you is valuable and it is used for price discrimination. So there are some market niches for privacy-enhancing technologies, but they are by no means the general solution to surveillance problems.[151]

157. Professor Anderson also argued against the use of digital identities as a way of protecting privacy on the grounds that they allowed organisations which hold personal information to shift responsibility for protecting that information on to the individual, as guardian of his or her identity:

> the rhetoric of identity becomes a means of passing the buck. In the old days, if someone went to the Midland Bank, pretended to be me and borrowed £10,000, that was impersonation and it was the bank's fault. Now, it is my identity that has been stolen, so it is supposedly my fault, and I end up having a furious row with the credit reference agencies. So the construction of the concept of 'identity' as something that belongs to me, that I have to protect with the help of government is not particularly helpful in this debate.[152]

We discuss identity management in the context of the Government's plans for identity cards below at paragraph 239.

158. Professor Anderson told us that a better approach to protecting personal information would be to begin by thinking about:

> the underlying business process of people, when they go to a government office, being dealt with in a fair and reasonable way; whether banks' transactions with their customers are regulated reasonably.[153]

Like Professor Anderson, Mr Bramhall emphasised the importance of processes in protecting privacy. These processes combined the technical aspects of designing systems for managing information, and the procedures used by organisations themselves:

> Those processes are as much to do with management practice as they are to do with technology and, by themselves, those processes require some technology to help them as well.[154]

> I do not think the issue is fundamentally one of the technology and its capability of addressing that issue; I think it is much more about education and awareness and people following good practice and, by that, I do not just mean the individual, but system designers following good practice.[155]

151 Q 204 (Professor Anderson)

152 Q 209 (Professor Anderson)

153 *Ibid.*

154 Q 204 (Pete Bramhall)

155 Q 209 (Pete Bramhall)

This approach would involve establishing clear routes to guidance for individual users and system designers, and means of redress for individuals whose personal information has been compromised.

159. **We welcome efforts to develop technological means by which organisations and individuals can protect personal information and prevent unwarranted monitoring of individuals' online activities. We recommend that the Government track and make full use of new developments in encryption and other privacy-enhancing technologies and in particular those which limit the disclosure and of collection of information which could identify individuals. We further recommend that the resources of the Information Commissioner's Office be expanded to accommodate sufficient technical expertise to be able to work with the Chief Information Officer to provide advice on the deployment of privacy-enhancing technologies in Government.**

160. **We recognise, however, that awareness of and access to privacy-enhancing technologies is not universal amongst the public. Over-reliance on the capacity of technology to secure data systems leads to neglect of the need to ensure that processes for the management of information by organisations are robust. It also raises unrealistic and potentially discriminatory expectations of individuals who are not in a position to take steps to prevent the theft of their personal information.**

161. **Where individuals have little or no choice about providing personal information, such as in their interactions with Government, it is especially important that the organisation which collects and holds the information takes responsibility for safeguarding it, rather than attempting to pass on the responsibility to the individual. The organisation's responsibility should begin before collection takes place: by obtaining consent for collecting and processing data where possible and by providing an explanation where this is not possible.**

162. **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. The Home Office should highlight the distinction between those areas in which individuals can exercise choice by giving or withholding their consent, and those areas in which seeking informed consent is not feasible and transparency is particularly important.**

163. **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 personal information. We recommend that the Government adopt a principle of data minimisation in its policy and in the design of its systems. We further recommend that the Government acknowledge the distinction between identification and authentication as one which is valuable in its efforts to adhere to this principle.**

164. **It is not just the volume of data collected that creates a problem: the longer information is retained, the more likely it is that the information will be out of date and inaccurate. Information should be held only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes**

rather than service delivery it should normally be anonymised and retained only for a previously specified period.

The case for new safeguards

165. Much of the evidence we received in our inquiry argued for new or strengthened safeguards for personal information and against unwarranted surveillance, on the grounds that:

- existing safeguards were not sufficient to meet the demands of new circumstances created by the growth in capacity and sophistication of private and public sector systems for collecting and storing information
- trends in terms of the public's willingness to give up information and the Government's enthusiasm for sharing it across departments gave rise to serious concerns
- criminal activity involving the abuse of databases and personal information stored in other ways had intensified.

Tackling abuse of databases through criminal activity or negligence

Criminal activity

166. A great many of those who submitted evidence to our inquiry raised concerns about the abuse of databases by criminals. Symantec told us that:

> Data is one of the most important assets of any organisation and a valuable target for attackers. Identity-related information is becoming a valuable asset to criminals, resulting in both public and private sector databases containing sensitive information [becoming] increasingly vulnerable to attack.[156]

Hewlett-Packard Laboratories referred to "the present level of cybercrime and likely continuation or steepening of its rate of increase".[157] The assessment of the Government's Chief Information Officer's was that:

> The more and more that the technology becomes sophisticated, we absolutely will be able to find people who are getting access to systems and using information illegally.[158]

167. Professor Ross Anderson also commented on recent developments in relation to criminal use of technology to steal personal information:

> The most recent innovations in crime have not been principally technological, but principally psychological because, as the technology gets better, so it becomes easier to deceive individuals, so we are seeing an enormous rise in phishing, in pretexting and other things that involves deceiving people. The criminals are not going to stop

156 Ev 156

157 Ev 178

158 Q 415 (John Suffolk)

> deceiving machines as well and we are going to see keystroke loggers, we are going to see the rise in pharming and we are going to see technical crimes going along with crimes that involve deceiving people.[159]

Pretexting

Pretexting involves impersonating someone, often using stolen personal data, to contact a business or individual in an attempt to gain access to information or money or to manipulate the business or individual in another way.

Keystroke logging

Keystroke logging is a method of recording what is typed on a keyboard, which can be used to capture passwords and other personal information.

Pharming

Pharming involves stealing information by diverting a genuine website's traffic to a bogus website designed to look and appear to function in the same way as the legitimate one.

168. The Finance & Leasing Association and Experian outlined the steps that the credit industry has taken to support victims of identity fraud, or identity theft as it is often called. On average, Experian said, 100 victims of fraud contact its dedicated team each week:

> By acting on a consumer's behalf and by co-ordinating any necessary activity the Experian service significantly reduces the amount of time it would normally take an individual to restore his or her credit history.[160]

The Foundation for Information Policy Research (FIPR) took issue with the term 'identity theft' and the measures in place to tackle the crimes described by the term.[161]

Increasing capacity to investigate and penalise criminal activity

169. FIPR argued that "action is needed to make the Information Commissioner's Office more effective and to make proper penalties available for abuse … the ICO has always been lacking in technical capability, which has undermined its credibility".[162] Symantec called for:

> an urgent review of the Information Commissioner's Office powers … in order to remove any existing limitations on the ICO's ability to investigate possible misuse of data and increase the legal and financial penalties for offences. Consideration should

159 Q 214 (Professor Anderson)

160 Ev 229

161 See above at paragraph 101.

162 Ev 226

also be given to the staff and resources currently allocated to the Information Commissioner to ensure the ICO's continued effectiveness.[163]

170. The Information Commissioner himself has sought support for a strengthening of his Office's powers to tackle criminal activity in relation to personal data. He told us that since embarking on his work to expose a black market in personal information he had seen "better penalties coming through from the courts using their existing powers" but noted that in the cases his office prosecuted criminals "often ended up with derisory penalties: a conditional discharge for one of the most serious ones, or very, very low fines".[164]

171. On 21 November 2007, the Prime Minister announced that the ICO would be given the power to "spot-check" government departments to ensure that they complied with Data Protection legislation.[165] He also announced that he had asked the Cabinet Secretary to undertake a review of the data handling procedures of departments and agencies. An interim progress report was published on 17 December 2007. The Ministry of Justice (MoJ) summarised the report's recommendations for data security and protection:

- ensuring that departments are clear about roles, responsibilities and minimum standards that they must apply
- reinforcing the culture across the public service that values and protects information and people's privacy
- ensuring that performance is transparent and the right to external scrutiny mechanisms are in place to promote improvements into the future.

The MoJ also outlined the report's initial recommendations in relation to the framework within which data is handled across Government:

- enhanced transparency with Parliament and the public about action to safeguard information and the results of that action, through departmental annual reports and an annual report to Parliament
- increased monitoring of information assurance through, for example, Accounting Officers' Statements on Internal Control
- improved guidance to those involved in data handling, that is simplified and better tailored, setting clear common standards and procedures for departments on data security
- legislative steps to enhance the ability of the Information Commissioner to provide external scrutiny of arrangements across the entire public sector through 'spot checks'
- commitment in principle to provide for new sanctions under the Data Protection Act for the most serious breaches of its principles.[166]

163 Ev 156

164 Q 59 (Richard Thomas)

165 HC Deb, 21 November 2007, col 1179

166 Ev 270

Providing for developments in data storage, sharing and searching

Information-sharing

172. At the outset of our inquiry we asked the Information Commissioner about developments in relation to information collected and held by the public sector. He responded:

> I think you have to start the debate by recognising that there is a lot of pressure now for more information to be shared across different parts of the public sector. Sometimes that is not particularly controversial or not particularly difficult. In relation to the information between the tax people and the social security people, most of the population expect that goes on already … The sharing of information between the tax authorities and the police authorities, or between the health authorities and the police authorities raises far more controversial and difficult issues … you have to take a case-by-case approach.[167]

> The Government talks about public services being more citizen-centric, and that is welcome, but is anyone seeing it from the point of view of the citizen in terms of all this information being collected and shared about them?[168]

173. The Information Commissioner has since developed a Framework Code of Practice for Sharing Personal Information. Published on 10 October 2007 the Framework explains how organisations can set up their own arrangements to ensure that where personal information is shared, good practice is adopted. It aims to help organisations decide when to share information and what information to share, highlights the consequences of sharing and deals with the issue of consent.

174. The Code is designed to be flexible, enabling organisations to adopt it wholesale or to extract some of its content and integrate this into existing policies and systems. The Information Commissioner's Office told us that this was the first time that a code which could be adapted and used to suit the needs of those involved in a particular information-sharing operation, had been developed:

> It reflects the fact that the range of situations in which information-sharing can take place is so broad that trying to develop a single prescriptive code … would be unworkable.[169]

175. Government departments take steps to safeguard databases and establish procedures for securing access to information by authorised staff, recognising that unauthorised access and other security breaches pose a risk. For example, the Department of Health's new electronic patient record system will be overseen by a National Information Governance Board, representing:

> an extremely high-level and visible statement of the accountability for information governance.[170]

167 Q 34 (Richard Thomas)

168 Q 40 (Richard Thomas)

169 Ev 258

Other safeguards include:

- a set of technical access controls and audit facilities that, along with the professional standards of staff in the NHS, safeguard sensitive patient information from inappropriate disclosure
- a comprehensive privacy statement in the form of the NHS Care Record Guarantee, articulating in plain language precisely what NHS organisations must do to meet legal and policy requirements
- the application of international security standards across all systems
- the operation of stringent security controls—such as vetting, use of smartcards and pass codes, proof of a "legitimate relationship" to a patient as a pre–requisite for access to records, setting standards for use of records through codes of conduct and professional responsibilities—to prevent unauthorised access to personal information and to detect potential abuse.[171]

176. The Department of Health acknowledged, however, that breaches of health databases were an ever-present danger:

> You cannot stop the wicked doing wicked things with information and patient data.[172]

"Audit trails" were used to identify abuse of databases and formal disciplinary procedures were in place to deal with individual members of staff involved in such breaches.[173]

177. The Department for Children, Schools and Families argued that for new databases such as ContactPoint, a clearly-defined purpose for the collection and sharing of information acted as a safeguard against 'function creep':

> I do draw a distinction perhaps between education and the care of and welfare of children, and when it comes to systems like ContactPoint there is very clear regulation in place … so I see no drift from that. ContactPoint is there for a very specific purpose and that is the backstop to what that system will be used for.[174]

178. The Department for Transport emphasised the importance of clarity in establishing the legal basis and purpose of requests for it to share data:

> we certainly do review the legal basis on which we do data-sharing. Most of our data-sharing is fairly long-standing but we would certainly want to know on what basis any approach was made to us and the legal justification … We need to look at it both

170 Q 327 (Richard Jeavons)

171 Ev 220

172 Q 334 (Richard Jeavons)

173 Q 327 (Richard Jeavons)

174 Q 352 (Tim Wright)

> from both ends of the telescope … have they got the power to seek the information but also have we got the power to give it".[175]

179. Whilst responsibility for the privacy aspects of individual policies rests with the departments which hold information, the Ministry of Justice works with departments to ensure that they comply with data protection legislation and to assist departments which propose to share information. MoJ considers the following issues to be "critical" in any decision on information-sharing:

> is there a purpose for sharing information; do the powers exist to share the information; is any intrusion on privacy proportionate to the benefits that will be gained from sharing the data; and is the data going to be adequately protected in terms of the principles underlying the Data Protection Act?[176]

'Walport Review'

On 25 October 2007 the Prime Minister asked Dr Mark Walport, Director of the Wellcome Trust, and Richard Thomas, the Information Commissioner, to conduct a review of the framework for the use of information in the private and public sector.

The review will:

consider whether there should be any changes to the way the Data Protection Act 1998 operates in the UK and the options for implementing any such changes

provide recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection

provide recommendations on how data-sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability[177]

A consultation on these issues was launched on 12 December 2007 and closed on 15 February 2008. A report and recommendations are to be submitted to the Secretary of State for Justice in the first half of 2008.[178]

Security breaches and data loss incidents: strengthening non-regulatory safeguards

180. The Information Commissioner works with private and public sector organisations, including Government departments, to ensure that the safeguards put in place by the Data Protection Act are complied with. The Commissioner told us that he had—by means of codes of practice and other guidance—enjoyed a degree of success in reducing the number

175 Qq 357–358 (Dr Stephen Hickey)

176 Q 394 (Clare Moriarty)

177 Source: http://www.justice.gov.uk/reviews/datasharing-intro.htm

178 Ev 270–1

of cases of abuse of surveillance technologies by organisations in some areas. One code of practice covered "all aspects of monitoring staff in the workplace": recruitment, personnel records, monitoring email and internet use and health checks. The Commissioner told us that whilst risks had not been eliminated:

> the fact that we were able to secure an agreed code of practice [with the support of the Trades Union Congress and the Confederation of British Industry]—we got agreement and we pushed this very hard around the employer community, and the trade unions have taken it seriously too—shows that in this particular context of the workplace—and data protection creeps everywhere, it is a horizontal law—the risks of excessive surveillance have been very substantially reduced because of our code of practice.[179]

181. A significant strand of the Commissioner's recent work to strengthen safeguards against excessive surveillance has been research into and development of guidance on Privacy Impact Assessments (PIAs). Envisaged in the first instance as a voluntary step by Government, PIAs would involve:

> An attempt by the organisation which is going to be collecting information in new or enlarged ways to record what they are going to do, why they are going to do it, how they are going to do it, to identify the various risks associated and to spell out publicly how they are going to mitigate those various risks. It is a discipline. It is a sort of risk management or risk assessment programme.[180]

The Commissioner emphasised that PIAs should not represent a "bureaucratic intervention".[181]

182. PIAs are a requirement for federal agencies in the United States. Mr J Trevor Hughes of the US-based International Association of Privacy Professionals, told us that those who were engaged in completing PIAs were:

> very supportive of and enthusiastic about such measures as a transparent tool not only for governmental data but for privacy professionals who use this tool to assist in the development, deployment and design of these products and services and allow citizens a way to look into the operations of their government to see how things are working.[182]

During our visit to the United States Hugo Teufel, Chief Privacy Officer at the Department of Homeland Security told us that PIAs were made available on the internet and that they had to be updated every two years, with a reassessment of the need for the systems and the information collected by those systems.

183. MITRE, a not-for-profit corporation which works for the US Government and other sponsors and specialises in systems engineering and information technology, undertook

179 Q 62 (Richard Thomas)

180 Q 69 (Richard Thomas)

181 *Ibid.*

182 Q 104 (J Trevor Hughes)

research into the development and use of PIAs. Members of MITRE's privacy team acknowledged that whilst PIAs should be integrated with the design stage of a project, too often they were not carried out until the end of the process, when it was more burdensome to resolve problems. When properly implemented, we heard, PIAs provided an iterative process for assessing privacy, which would help to ensure that privacy concerns played a substantial part in the design of any system, and a 'gatekeeper' stage which would prevent a project going ahead until the PIA documentation had been approved.

184. Dr Ian Forbes of the Royal Academy of Engineering was more sceptical of the value of PIAs as a safeguard against the risks posed by security breaches or excessive surveillance. He argued that in their current form PIAs were not thorough risk assessments but rather that:

> Mostly they seem to be compliance statements or best practice statements. I do not think any of them actually say, "This is your privacy and this is how it will impact upon it for good or ill".[183]

The Royal Academy of Engineering argued in its written evidence that:

> PIAs may be useful in ensuring that government policies and their implementation do not infringe excessively on people's privacy. However, it is by no means certain that they will prove effective and they may well hinder the development of ICT projects.[184]

Security breaches and data loss incidents: calls for more stringent regulation

185. The Information Commissioner argued for an extension of his powers of audit and inspection under the Data Protection Act, in order better to tackle both illegal activity and weaknesses in the steps taken by organisations to protect the information they hold. Whilst he saw "self-interest at work" as organisations were "working very hard" to prevent breaches, the Commissioner told us that there was also "a lot of complacency". The ICO found that "people are really quite shocked to find out how easily their systems have been breached".[185]

186. The Commissioner also called for further regulatory safeguards to prevent security breaches caused by poor information-handling practices, with penalties where there is a flagrant or a negligent or repeated disregard of the requirements of the law. The Commissioner said:

> I do not want to prosecute left, right and centre, but I would like there to be a deterrent and, in the extreme case, where there had been unacceptable disregard of the regulations, to be able to go to court and have a system of fines to sanction that behaviour.[186]

183 Q 268 (Dr Forbes)

184 Ev 165

185 Q 68 (Richard Thomas)

186 Q 64 (Richard Thomas)

187. Professor Anderson argued that privacy was largely a policy matter rather than a technology matter because "privacy intrusions generally stem from the abuse of authorised access by insiders or from failures to regulate such access properly".[187] He linked security breaches not with inadequacy of technological safeguards but with a lack of incentive to protect information:

> One of the things that we have learnt over the past six or seven years is that, when systems fail, they largely do so because incentives are misaligned and classically because some of the persons who guard a system are not the persons who bear the full economic costs of failure.[188]

Conclusion: curbing unnecessary surveillance and protecting privacy

188. The Home Office says that it takes a "proactive approach to protecting information". As part of its reform programme the Home Office developed a corporate strategy for information, systems and technology which recognised information assurance as "one of the top cross-cutting themes". In August 2007 the Home Office initiated an information assurance review which it expects to be completed by March 2009, in line with its implementation programme for the Cabinet Office review of data handling procedures in Government.[189]

189. **We welcome the reviews commissioned by the Government to improve data security, particularly in relation to information-sharing. We expect the Government to make full use of the opportunity these reviews provide to reassess the adequacy of the definitions and principles set out in the Data Protection Act. Such a reassessment should be carried out not only in light of recent data loss incidents but also against the challenges presented by increases in the collection, storage and sharing capability of information systems and intensification in criminal activity associated with the misuse of personal information. The Home Office must act as a matter of urgency to tackle these challenges.**

190. **Any increase in the collection and storage of information increases the risk that security will be breached and that information will be used for purposes other than those for which it was collected. In keeping with a principle of data minimisation, more rigorous risk analysis of systems already in place must be carried out before new techniques for collecting information are deployed or new databases planned. The decision to create a major new database, share information on databases, or implement proposals for increased surveillance should be based on a proven need.**

191. **We commend the Information Commissioner for his work on Privacy Impact Assessments and support his drive to ensure that Government and others undertake thorough evaluation work in relation to the benefits and risks of surveillance. We also acknowledge that if published, in providing individuals and interest groups with details about surveillance activities which would not otherwise be made available, PIAs could**

187 Q 195 (Professor Anderson)

188 Q 186 (Professor Anderson)

189 Ev 274

help to raise awareness of the issues the Information Commissioner has sought to highlight.

192. **We are concerned, however, that PIAs might be regarded simply as bureaucratic exercises, and that they would be undertaken not before and during the design phase of any system but afterwards; by which time their value as a practical risk assessment tool would have been lost. For PIAs to be effective they should be used to carry out preliminary risk analysis for a new project before the design phase begins. For Government departments and agencies this preliminary risk analysis should culminate in a summary statement, to be signed off by the Information Commissioner or otherwise subject to independent audit. The statement should set out the benefits of a new system against the risks posed by collecting, storing and using the information required by the system.**

193. **Every system for collecting and storing personal information should be designed with a focus on security and privacy. The design process should involve planning not only in relation to the technical aspects of access to systems but also to the staff management protocols for access and information-handling.**

194. **Every system for collecting and storing data is susceptible to unauthorised access, misuse and theft. For existing and proposed systems the Government should specify what it considers to be an acceptable level of failure and develop contingency plans to mitigate the damage caused by leaks or theft of data.**

195. **The weakest aspect of a system may be the establishment and enforcement of protocols for access and use rather than any technological safeguard. Organisations which manage such systems must take full responsibility for limiting access to databases and the information they contain and for enforcing procedures for sharing and transferring data. We support the Information Commissioner's call for an extension of his inspection and audit powers to facilitate the strengthening of these procedures across Government and the private sector. Tougher penalties for negligent information-handling should be introduced in order to make clear where the burden of responsibility lies.**

196. **A privacy officer or director of data security should be assigned by departments to take responsibility for risk analysis and to report to the Permanent Secretary on the privacy implications and safeguards of each project which involves the collection or sharing of personal information.**

197. **The Home Office should publish a report on an audit of the data collections managed by the Department and its agencies, outlining as far as possible without compromising security the technological and procedural safeguards currently in place.**

6 What role does surveillance play in the work of the Home Office and the fight against crime?

Introduction

198. We have attempted to examine the benefits of various forms of surveillance alongside the risks involved. Our conclusion is that any decision to collect information about people's activities should be taken only after an appropriate balance is struck between the potential harm, including intrusion of privacy, and intended benefit of the project. In considering databases and other forms of surveillance with a direct relevance to the fight against crime striking this balance is particularly important.

199. The benefits to the police and other security and law enforcement agencies in their work to prevent and investigate serious crime and protect the public can far exceed those of surveillance for other purposes. But the consequences of decisions made on the basis of inaccurate information or wrong assumptions or of a leak of information are more serious. Moreover, where surveillance has to be carried out without the consent or knowledge of the individual, it is more intrusive.

200. The Information Commissioner compared the risks associated with the collection of information by the private sector and surveillance carried out by the Government:

> I think there are commercial and other pressures impacting on the private sector which I see being taken very seriously indeed. The state has a monopolistic and often a mandatory power over citizens and it can do things without their consent, without their agreement, without their involvement for perfectly good reasons. The state has, if you like, greater potential but also can cause greater harm if people are wrongly labelled, if they are wrongly identified, if mistakes are made. Also the state tends to have larger numbers. The databases run by the state are much, much larger, so if things go wrong within a public sector database the effects would be multiplied many times more.[190]

The Commissioner's view, "broadly speaking", was that surveillance in the areas of responsibility of the Home Office and the Ministry of Justice represented the "most difficult challenge":

> for understandable reasons, people are collecting and using information. But this is where there are the most coercive powers against the citizen, and that is where … sometimes the importance of upholding liberties means that an independent commissioner has to say things which may be unpopular in the short term.[191]

190 Q 78 (Richard Thomas)

191 *Ibid.*

Home Office responsibilities in relation to the collection and sharing of information

CCTV or camera surveillance: proving the benefits and practising restraint

201. Reaction to the development of camera surveillance technology and proliferation of cameras themselves has come to represent the debate on surveillance in general: whilst its use and further development is accepted without question and welcomed in some quarters, to others it symbolises the worst excesses of a surveillance society.

202. The Information Commissioner told us that "the population like cameras and cannot get enough of them".[192] We did, however, hear evidence of some concern amongst the public about the use of cameras and about the regulation of the circumstances in which surveillance cameras are used. R.A. Collinge wrote to us to argue that "criteria need to be developed to decide how and when both public and private surveillance of this nature is essential and has real value".[193]

203. The Information Commissioner has sought to provide guidance on responsible use of camera surveillance. His CCTV code of practice (revised and reissued in 2008) is designed to help organisations comply with the Data Protection Act and to help them assure the public that they are using CCTV responsibly.[194] The Assistant Information Commissioner told us that the decision to install surveillance cameras should not be taken lightly:

> the actual assessment procedure, in deciding whether to establish a scheme, should be very, very rigorous. It should not just be on the basis of public popularity, or the technological capability to do it, or the financial capability to do it.[195]

Dr Ian Forbes of the Royal Academy of Engineering said that at present camera surveillance is used principally by those who want to "prevent, monitor and sometimes punish certain behaviours". This led, he believed, to "serious concerns", both about general invasions of privacy, and about the specific problems associated with predictive profiling of some sectors of the community.[196]

The case for camera surveillance

204. The Surveillance Studies Network noted the findings of a Home Office research study that the 13 CCTV schemes it assessed had "little overall effect on crime levels" and queried levels of investment by the Home Office in CCTV installation. The Surveillance Studies Network's report said that £500 million of public money had been invested in CCTV over

192 Q 24 (Richard Thomas)

193 Ev 129

194 Information Commissioner's Office, *CCTV Code of Practice: Revised Edition*, 2008

195 Q 24 (Jonathan Bamford)

196 Ev 241

the last decade and that during the 1990s the Home Office spent 78% of its crime prevention budget on installing CCTV.[197]

205. The Home Office stated in its written evidence for our inquiry that "Police experience and research studies show that CCTV has considerable crime detection potential, when used as part of a wider strategy".[198] Technological developments in camera surveillance increase this potential. Chief Constable Peter Neyroud of the National Policing Improvement Agency (NPIA) told us that in certain contexts facial recognition techniques could be "very effective in narrowing down the identification" of suspects and that "behavioural matching, the ability to pick out odd behaviours in a crowd" "might be particularly powerful in the case of counter-terrorism or a variety of street crimes".[199]

206. Assistant Chief Constable Nick Gargan of the Association of Chief Police Officers (ACPO) told us that he thought that the case for CCTV cameras was "compelling". He argued that CCTV material provided an "indispensable investigative tool":

> very often the first investigative action, or one of the very first investigative actions that takes place in virtually any serious crime inquiry or missing person inquiry or many other types of inquiry would be to conduct a trawl of CCTV evidence and see what that tells us.[200]

Chief Constable Neyroud said that whilst his view was that not enough research on the effectiveness of CCTV in the investigation of crime had been done, his "guesstimate" was that "we are getting almost as many detections, either directly or indirectly, from CCTV as we are getting from DNA and fingerprints". He also told us that CCTV was "crucial" in helping the police to find vulnerable missing persons.[201]

A lack of evidence?

207. The effectiveness of camera surveillance in the prevention of crime in particular has been called into question by the Surveillance Studies Network and the Royal Academy of Engineering amongst others. Professor Ross Anderson of the Foundation for Information Policy Research (FIPR) referred to work undertaken in connection with FIPR's report for the Information Commissioner on children's databases, which looked at a range of crime reduction initiatives:

> Yes, there may be some placebo effect from having large numbers of closed circuit television cameras around, but the analysis of the crime statistics which we cite tends to show that although they are good at reducing crime in car parks they are not so good at reducing crime in town centres and there is a very serious question about

197 Gill and Spriggs, Assessing the Impact of CCTV (London: Home Office Research, Developments and Statistics Directorate, 2005), pp 43, 60–61; Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript*, March 2007, p 19, para 9.5.3

198 Ev 192

199 Q 454 (Chief Constable Neyroud)

200 Q 444 (Assistant Chief Constable Gargan)

201 Q 456 (Chief Constable Neyroud)

> whether far too much money has been spent on these and not enough money on other crime reduction initiatives.[202]

208. Assistant Chief Constable Gargan said that it was "amazing how little impact" cameras seemed to have on "the behaviour of all but a very few individuals who are very conscious of the cameras and play up to those cameras. Chief Constable Neyroud argued that whilst it was a benefit "often missed in the studies", there was "quite reasonable evidence" that cameras:

> encourage people to use public space … create a capable guardianship of that space simply by their presence.[203]

The Minister of State for Security, Counter-terrorism, Crime and Policing, Rt Hon Tony McNulty MP shared this view. He acknowledged a paucity of evidence on the effectiveness of camera surveillance in the prevention of crime but was convinced of its value:

> Can I point to a definitive national study that quantifies in any way its success as a deterrent? No, I cannot, but I am sure everyone can come up with significant local and anecdotal evidence to suggest that, as part of an array of other measures, it is successful, not just as a deterrent, not just in terms of bringing public spaces back into public use but also, crucially, as an investigatory tool for the police.[204]

209. In May 2008 comments made at a Conference by Detective Chief Inspector Mick Neville of the Metropolitan Police's Visual Images, Identifications and Detections Office (Viido), received a great deal of media attention. DCI Neville is reported to have said that although "billions of pounds has been spent on kit", "only 3% of crimes were solved by CCTV": how the police would use the images captured and how they would be used in court were not issues that had been considered and there was no "fear of CCTV" because people thought that "the cameras are not working".[205]

Making camera surveillance more effective and increasing transparency

210. Much of the material captured by CCTV is currently of limited use to the police. Assistant Chief Constable Gargan confirmed that anecdotal evidence gathered by ACPO and the Home Office suggested that that "over 80% of the CCTV footage supplied to the police was far from ideal".[206]

211. In October 2007 the Home Office and ACPO published a National CCTV Strategy with 44 recommendations—on aspects such as standards and governance; registration, inspection and enforcement; training; storage volume and retention; and emerging technologies—on which it was felt that progress was needed "if we are to realise the full

202 Q 231 (Professor Anderson)

203 Q 457 (Assistant Chief Constable Gargan; Chief Constable Neyroud)

204 Q 506 (Rt Hon Tony McNulty MP)

205 "CCTV boom has failed to slash crime, say police", *Guardian*, 6 May 2008

206 Home Office/ACPO, *National CCTV Strategy*, October 2007, p 12

potential of CCTV across a varied range of uses and continue to receive the support of the public".[207]

212. Assistant Chief Constable Gargan told us that the strategy focused "specifically and particularly" on the 30,000 local authority-operated street cameras in England and Wales. He underlined the strategy's aim of bringing about a "gradual upgrading of facilities and a convergence of facilities towards a technical standard" so that more CCTV material could be useful to the police. Endorsing the assertion that the only people who should fear CCTV were those who engaged in criminal activities, Assistant Chief Constable Gargan called for CCTV material to be made more readily available to the police "because everybody knows it is there and we should not be hampered in our use of it".[208]

213. Chief Constable Neyroud argued that concerns about CCTV could be addressed by the development of standards, as part of an effort to increase the transparency of procedures relating to camera use:

> It is all part of the piece of being able to explain what it is there for, what its effectiveness is, how we are looking after it, whether the standards are moving on, the techniques that we are applying and who is applying them.[209]

214. Others who gave evidence to our inquiry called for a more participatory role for those under surveillance, giving a degree of control to individuals by allowing them to participate in the process of surveillance. The Foundation for Information Policy research argued for "equality of arms" in access to data:

> At present it is very easy for the police to get hold of CCTV data or ANPR data to prove that you did something bad, but it is a lot more difficult for you to get hold of it to provide that you did not, to establish an alibi.[210]

Jonathan Bamford, Assistant Information Commissioner, told us that transparency about where and how cameras were being used was important but that it could be difficult to achieve, particularly for motorists:

> Maybe we need to be slightly more creative there in trying to actually come up with solutions which help the public work out who is involved in the surveillance. One simple solution might be to create a website which has the road network on it; we are all used to mapping technology now, route planning; and you could click on that and actually find out who is involved in the surveillance at a particular point in time.[211]

215. The Royal Academy of Engineering's report on surveillance argued that making footage from CCTV cameras freely available to the public through the creation of "community webcams" would redress the imbalance of power between those in front and

207 Home Office/ACPO, *National CCTV Strategy*, October 2007, p 6

208 Qq 447–50 (Assistant Chief Constable Gargan)

209 Q 455 (Chief Constable Neyroud)

210 Q 232 (Professor Anderson)

211 Q 24 (Jonathan Bamford)

those behind the cameras by making organisations and individuals who use the information as accountable as those being filmed:

> Community members could object if they felt particular cameras were unnecessary or unnecessarily intrusive. This would limit the potential for voyeuristic or prejudicial misuse of surveillance.[212]

216. During our visit to the United States we discussed the use of camera surveillance in the state of Maryland. We heard from Governor Martin O'Malley and his staff that police in Maryland sought to engage the public in their work. Each police commander responsible for the installation of cameras was required to produce a public strategy and to work with the public before, during and after the installation of cameras. Steps such as setting out the aims of installation, inviting people to control centres to sit alongside police officers and watch the footage, and consulting with community leaders, could help to allay fears that the Government was simply 'watching' the public. Having won the trust of the community in this way, the police would rely on local people as a valuable source of intelligence.

217. Dr Ian Forbes told us that whilst the message sent out by the proliferation of cameras—"we are watching you, do not misbehave"—was "incredibly negative and critical",[213] attention should be paid to the positive uses of surveillance technology. Ordinary citizens should be given "an active stake and a determining say in the processes and practices of camera surveillance", to enable "new and socially beneficial uses of these surveillance technologies". He proposed that:

- The right to conduct surveillance should generate reciprocal rights for those under surveillance
- Purposes, placement, conditions of use, operating practices and personnel should, by law, be subject to consultation, agreement and challenge by those under surveillance.[214]

218. We put some of these proposals to our police witnesses. Chief Constable Neyroud made a distinction between cameras "we are overtly telling the public about because they are the cameras that are surveilling public space" and cameras on the road network which "are designed to catch people who are doing things that are illegal". He told us that whilst he had "less difficulty" with public access to the first kind of camera, he could not support "from a counter-terrorist point of view, providing Al Qaeda with a camera-free route map" which would diminish the effectiveness of the network of cameras on the roads.[215] Assistant Chief Constable Gargan said that public access to fixed cameras giving views of particular locations was "fine" but that local authority-run CCTV cameras were "quite a different story":

212 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, March 2007, p 49

213 Q 261 (Dr Forbes)

214 Ev 241

215 Q 460 (Chief Constable Neyroud)

> If, for example, the camera in Warwick High Street is focused on a jewellers half way down the High Street, it is probably doing that for a reason, and that information could be very valuable to the criminal who is thinking about robbing that jeweller later this morning.[216]

Ground rules for camera surveillance: data minimisation

219. When we challenged the Minister on the amount of information gathered from different sources, including cameras, about individuals, he argued that a great deal of data captured by cameras was "very temporary":

> The notion that somehow every product of an ANPR camera or a CCTV camera or any other aspect of government databases are all in some huge warehouse or shed somewhere with a live feed going in on a realtime basis, accessible to anyone across the State, central or local, simply is not the case. In many cases many of the CCTV cameras you are looking at and observing on the high street are on a sort of digital loops that will last days, no longer. Some go to live feed.[217]

> In any street you go down at least half the cameras or more will be private rather than public anyway, and many of those in the public domain will be on a very short feed, and the notion that they are just storing up all of this data at the end of the day, shipping it off to MI5, the police or anything else is profoundly wrong and not the case. Were that the reality then I would share some of the concerns of those who talk about a surveillance State, but it is not, so I do not.[218]

The Minister insisted that data protection concerns and "the rules and regulations surrounding what we do and how we do it" were "uppermost in the Government's mind" in relation to CCTV and "all aspects of surveillance".[219]

220. However, the Information Commissioner shared with us his concerns that developments in surveillance camera technology might lead to more information about individuals' activities being collected. Although he acknowledged that CCTV could provide "public reassurance" he told us that he resisted attempts to move beyond the collection of images:

> There is a debate starting now as to whether there is a case for the authorities to place microphones on the streets, and our instincts are very, very hostile to that idea. We think that would be unacceptable.[220]

221. **Under camera surveillance in public spaces, individuals have very little control over whether or not their images and movements are captured and over how they are stored and used. This lack of choice intensifies the obligation on camera operators and regulators to behave responsibly and to deploy surveillance technology only where it is**

216 Q 460 (Assistant Chief Constable Gargan

217 Q 495

218 Q 509

219 *Ibid.*

220 Q 24 (Richard Thomas)

of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty.

222. **We acknowledge the popularity of CCTV schemes and do not underestimate the potential effect on crime levels of successful attempts to encourage people to use public spaces. However, as the Minister told us, it has been difficult to quantify the benefits of CCTV in terms of its intended effect of preventing crime. We recommend 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.**

223. **We welcome the drive to create standards for the use of camera surveillance in order to enhance the value of the images captured in the fight against crime. We recommend that the Home Office work with the police to increase public awareness and manage public expectations of camera surveillance.**

224. **Whilst we share the reservations of the police about unfettered public access to surveillance cameras, we endorse the Information Commissioner's calls for greater transparency in relation to camera surveillance and recommend that the Home Office take steps to facilitate access to footage in certain circumstances, for example where an individual is seeking to eliminate him or herself from police enquiries.**

225. **The continued value and popularity of CCTV depends on continued public confidence that camera operators are acting responsibly and that the Government, in regulating CCTV schemes, is mindful of concerns about privacy. We note that the Minister saw the fact that much CCTV footage is held for a limited period of time as a barrier to the development of a surveillance state. In designing camera schemes operators should consider how long images need to be stored and the Home Office should support a principle of data minimisation in this respect.**

226. **We acknowledge that technological developments have significantly increased the potential of camera surveillance in terms of crime detection. However, the Government should evaluate the impact of each major development for its effect on individual liberty. In particular, the Home Office should give its assurance that it will not countenance schemes such as those which involve the use of microphones attached to cameras, and in effect apply the techniques of directed and intrusive surveillance to the general public. Such measures impinge on the degree of privacy individuals expect to be able to enjoy in public spaces and the Home Office must take responsibility for guarding against this kind of constraint on individual liberty.**

Identity cards: reducing the risks

Purpose of the scheme: the prospect of 'function creep'

227. We did not set out in this inquiry specifically to follow up our predecessor Committee's work on identity cards,[221] but rather to explore selected strategic issues in the context of concerns about the collection, storage and use of personal information by the Government. The Home Office told us that the National Identity Scheme—identity cards and the National Identity Register which is to underpin the card system—is "not designed as a surveillance tool" but rather that its purpose is to:

> protect individuals' identities from abuse and provide a secure way for people to prove their identity more reliably, helping to tackle illegal immigration, crime and terrorism as well as improving public services.[222]

228. In announcing the publication of the *National Identity Cards Scheme Delivery Plan* the Home Secretary reiterated these benefits:

> The Government's National Identity Scheme means that for the first time UK residents will have a single way to secure and verify their identity. We will be able to better protect ourselves and our families against identity fraud, as well as protecting our communities against crime, illegal immigration and terrorism. And it will help us to prove our identity in the course of our daily lives—when travelling, for example, or opening a bank account, applying for a new job, or accessing government services.[223]

The Delivery Plan lists security controls for the Scheme and emphasises similarities between the information to be recorded on the National Identity Register and that stored on the passport database.[224] In an evidence session on data security issues in relation to identity cards, Meg Hillier MP, Parliamentary Under-Secretary of State told us that:

> The information on the identity card will be much the same as the information that is on the current passport, the readable zone. The information on the database will include National Insurance number, update of address and a log of who has ever looked at the record. I think it is just worth nailing, Chairman, as it was raised, this idea that there is going to be a lot of different information. This information is routinely provided by people to government and it is just going to be held in one place.[225]

229. During our inquiry we heard evidence from those who took issue with the scheme on the grounds that identity cards would serve to increase the Government's capacity for surveillance and that, as another Government collection of data, the National Identity Register would serve to increase the risk of a security breach. The LSE's Political Science

221 Home Affairs Committee, Fourth Report of Session 2003–04, *Identity Cards*, HC 130

222 Ev 193

223 "National Identity Scheme Delivery Plan published", Identity and Passport Service pres release, 6 March 2008

224 Home Office, *National Identity Scheme Delivery Plan*, March 2008, p 13

225 Evidence taken by the Committee on 26 February 2008, HC 365-I, Q12

Identity Project asserted that the ID Cards scheme is designed to maximise the surveillance capabilities of identity cards, arguing that "the process of enrolment into the Scheme involves bringing together data from a dispersed set of existing databases".[226]

230. The Project pointed out that a great many countries have made "very different design decisions about the collection and use" of the kind of personal data to be included in the National Identity Register. France, for example, has introduced a central database for ID cards but it is limited only to the delivery of the card system and German law prevents the creation of the kind of central database envisaged for the UK. Information is stored locally and destroyed after cards are issued.[227]

231. Several of our witnesses raised concerns about that 'function creep' would expand the ambitions of the National Identity Scheme beyond the purposes set out by the Home Office. Dr Chris Pounder's evidence charted the development of the Scheme and its links with the Citizen Information Project, which evaluated how public money could be saved, and services to citizens improved, by increasing the sharing of basic citizen information (contact details such as name, address and date of birth) across central and local Government. Dr Pounder argued that the Identity Cards Act made provision for extension of the uses of the information held on the National Identity Register. Specifically s1(4)e of the Act provides for the Register to be used for a general public administration purpose, and more generally, Dr Pounder told us:

> legislative powers which impact on the processing of personal data are often needed to provide flexibility as to how the processing of personal data is to occur, or to allow for the use of the techniques or technology not yet designed…To introduce a degree of flexibility, widely drawn powers are defined and this exacerbates the risk of function creep or use of powers by a future Government in a different context.[228]

Liberty also objected to the National Identity Register on these grounds:

> If the NIR comes into existence then it is likely to make logistical, financial and political sense to increase the purposes it serves. If, for example, the NIR had been in operation at the time of Ian Huntley's conviction for the Soham murders, the mood of public outrage was such that there would have been political pressure to place details of convictions or 'soft' non conviction police intelligence onto NIR entries. 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.[229]

232. The Information Commissioner told us that his office had had "some dialogue" with the Home Office and the Identity and Passport Service about the implementation of the National Identity Scheme. He told us, however, that he had not been made aware of an

226 Ev 135

227 Ev 137

228 Qq 317–318 (Dr Pounder); Ev 113

229 Ev 189

important change to the National Identity Register (the use of information from the Department for Work and Pensions) until it was publicly announced.[230]

233. We asked the Minister specifically about the intended benefits of the National Identity Scheme in relation to crimes such as terrorism, illegal immigration and e-crime, in the context of the Government's argument that the introduction of identity cards represented an effective way of preventing identity fraud. Whilst Mr McNulty said that there was no "quintessential, comprehensive, all-singing, all-dancing, quantitatively, mathematically robust, cost-benefit analysis" of these functions of the National Identity Scheme, he was confident that "significant cost-benefit analysis work" on the intended benefits of the Scheme in relation to crime had been "put into the public domain" "over the course of time".[231]

234. The Information Commissioner acknowledged that the holding of information on separate databases (managed by the Department of Work and Pensions and the Identity and Passport Service) provided some safeguards for individual privacy but warned that collecting more information increased the risk that a comprehensive picture of an individual's activities could be developed:

> Whether using the National Identity Register or by other means, as you go down this route of drawing all the threads together then incrementally the big picture builds up … the Government talks about public services being more citizen-centric, and that is welcome, but is anyone seeing it from the point of view of the citizen in terms of all this information being collected and shared about them? The National Identity Register could—I emphasise, could—undermine public confidence in this collection of information.[232]

235. The information collected for the National Identity Register will include National Insurance numbers, addresses and "a log of who has ever looked at the record".[233] This log, intended to regulate access to the information on the Register, could also serve, the Information Commissioner told us, to track individuals' activities:

> We have always expressed anxieties about what is called the data trail. It can be an audit trail. We recognise that there is a tension there, but the more that information is kept about every transaction with your card, every time your details are searched, the greater the risk in surveillance terms for individuals. That does begin to build up a very comprehensive picture, available to the state about your activities, which people may not be at all comfortable about.[234]

230 Q 39 (Richard Thomas)

231 Q 540–1

232 Q 40 (Richard Thomas)

233 Evidence taken before the Committee on 26 February 2008, HC 365-i, Q11

234 Q 39 (Richard Thomas)

The Commissioner also voiced reservations about the "quality of imported data" from the Department for Work and Pensions, which, he said, "has not had what one might call a completely clean database in the past".[235]

236. **We have not sought in our inquiry to revisit the debate on the merits of identity cards. We are concerned, however, about the potential for 'function creep' in terms of the surveillance potential of the National Identity Scheme. Any ambiguity about the objectives of the Scheme puts in jeopardy the public's trust in the Scheme itself and in the Government's ability to run it. Whilst we accept the Government's assurance that the Scheme will not be used as a surveillance tool, we seek the further assurance that any initiative to broaden the scope of the Scheme will only be proposed after consulting the Information Commissioner and on the basis that proposals will be subject to parliamentary scrutiny in draft form.**

237. **We recommend that the Home Office produce a report on the intended functions of the National Identity Scheme in relation to the fight against crime, containing an explicit statement that the administrative information collected and stored in connection with the National Identity Register will not be used as a matter of routine to monitor the activities of individuals.**

Securing the National Identity Register

238. In its *Strategic Action Plan for the National Identity Scheme* the Home Office said that "the success of the National Identity Scheme in delivering its benefits relies on public confidence, especially in the accuracy and security of the information held in the National Identity Register".[236] The Plan outlined a range of security measures for protecting information, including the decision that the different types of information to be recorded and linked by the National Identity Register—biographical details, biometric information, and administrative data such as details of the card issued to an individual—will be stored separately, on the Department for Work and Pensions Customer Information System (CIS), and existing Identity and Passport Service systems.[237] The Scheme is to be overseen by an Identity Scheme Commissioner, who will make reports (which will be laid before Parliament) to the Home Secretary.

239. Following the loss of child benefit data from Her Majesty's Revenue and Customs Members of both Houses asked questions about the security of the National Identity Scheme. Lord West of Spithead told the House of Lords that:

> Her Majesty's Government remain committed to the implementation of the National Identity Scheme, including the issue of identity cards and establishing a National Identity Register. The National Identity Scheme will be security accredited to the highest standard necessary and, as the National Identity Register is not yet in

235 Q 39 (Richard Thomas)

236 Home Office, *Strategic Action Plan for the National Identity Scheme: Safeguarding your identity*, December 2006, p 13

237 Home Office, Strategic Action Plan for the National Identity Scheme: Safeguarding your identity, December 2006, p 11

> place, we will be able to learn any lessons from the HM Revenue and Customs incident.[238]

Ministers rejected the suggestion that the National Identity Scheme should be delayed or abandoned in light of concerns raised about the Government's handling of personal information following the data loss incidents in 2007 and 2008. The Government's arguments focused on the use of biometric information to verify identity and prevent identity fraud.

240. In a debate in Westminster Hall Meg Hillier MP emphasised the biometric element of the National Identity Scheme and alluded to a link between the collection of information and trust:

> Once we have identity cards that lock a biometric fingerprint and a facial image into a digital chip which can then be checked to prove that the person is who they say they are, and by protecting the data we will have a much more secure system. We will no longer have to rely on trust, which we have—unfortunately—relied on happily for a long time. Trust is no longer enough to protect against identity fraud.[239]

When we took evidence on data security in relation to identity cards, the Minister, Meg Hillier MP, argued that "there are quite big differences between that data [lost by HMRC] and the National Identity Register" and outlined the safeguards for information held on the Register, emphasising their basis in established practice:

> The National Identity Register, essentially, will be a secure database; it will not be accessible online; any links with any other agency will be down encrypted links. The only physical transfer, for the most part, will be for disaster recovery, just as we do currently with the Police National Computer, just as we do currently for the passport database, for example, and there will be very, very limited access to other jurisdictions within Europe, but, again, the sort of thing we are currently doing.[240]

241. The Minister later acknowledged, in noting that the data loss by HMRC had been caused by "a human error", that limiting access to the information on the Register was a key factor in securing it:

> we are assessing the risk and are taking proportionate action to make sure that human error potential is as limited as possible by having fewer than 100 people with access to the actual database, just as with the Police National Computer—there are very few there.[241]

The Minister noted that biometric and biographical information would be held on separate databases and that the link would be made when an individual "allows verification of their

238 HL Deb, 7 January 2008, col 181WA

239 HC Deb, 5 December 2007, cols 279–80WH

240 Evidence taken before the Committee on 26 February 2008, HC 365-i, Q1

241 *Ibid.*, Q 17

identity". She told us that this step amounted to "putting the power … in the hands of the individual".[242]

242. Individuals who allow verification of their identity, however, do so on trust: they rely on the Government to secure the biometric data they have given to the National Identity Register. Our predecessor Committee and more recently the UK Borders Bill Committee have heard evidence on the efficacy and security of large databases of biometric information. Ross Anderson, Professor of Security Engineering at Cambridge University, told the UK Borders Bill Committee:

> There is a fundamental security engineering problem with biometrics as opposed to, say, the cryptographic keys in your chip and PIN card. Once your biometrics become compromised, you cannot revoke them; it is not practical to do eye or finger transplants. Therefore, once you start using biometrics on a very wide scale, for all sorts of everyday transactions, the mafia—for want of a better word—will also have your biometrics. You do not know which shops are owned by the mafia, but if you end up having to put your fingerprint on the glass every time that you buy a can of Coke, sooner or later the mafia will have the biometrics of millions of people.[243]

243. Doubts have also been raised about how effective—if registration on the National Identity Register becomes compulsory—a means of identification biometrics will provide for the entire population. According to Professor Daugman of the University of Cambridge, owing to the false match rate associated with fingerprints, a fingerprint-only database could not "deliver the goal of one citizen, one identity, because it cannot survive so many comparisons without making false matches—so there will be false claims of multiple identities".[244]

244. Iris scans produce more accurate results and are more difficult to forge than fingerprints. However, Meg Hillier told us that although the Government was not "ruling out iris technology for ever", it would not form part of the "first generation" of identity cards or biometric passports. In discussing the security of databases of biometric information, Tony McNulty argued that a key factor was the introduction of the National Identity Scheme in "very incremental fashion":

> both the security of it and the efficacy of the IT software access and all the other elements will be learned and relearned on an evaluative curve and feedback loop at each stage. We have quite deliberately eschewed the notion—not least I would guess in passing because the most lamentable of government IT projects are those that are Big Bang and you switch from one system to another straight away and not least because of the importance of security and other aspects—of going full on for introducing things in one big hit, so there will be incremental lessons learned on security, on access, on the architecture and on the efficacy at every stage of the implementation of the programme.[245]

242 Evidence taken before the Committee on 26 February 2008, HC 365-i, Q 1

243 Public Bill Committee, 1 March 2007 (afternoon), Q 215

244 "ID cards will give 'false' data", BBC News Online, 31 July 2007

245 Q 548

The Minister told us that the Government did not plan to publish any sort of privacy impact assessment for the Scheme unless "any subsequent move to a compulsory registration" was made.[246]

245. **We note the distinction drawn by the Minister between the National Identity Scheme and "the most lamentable of government IT projects" and agree that staged implementation provides a degree of protection against security breaches. Nevertheless, the Home Office must plan for security breaches and in particular it should examine the consequences of theft of the biometric information which forms part of the NIR.**

246. **Taking into account the effect of recent data loss incidents on public confidence in the Government as a guardian of personal information, we recommend that the Home Office submit more detailed plans for securing the NIR databases and a broad outline of contingency plans to be implemented in the event of a loss or theft of biometric information from databases managed by the Identity and Passport Service, for comment by the Information Commissioner.**

247. **Recent data loss incidents have involved failures not of technology but of policy in that those who had access to the information in question did not observe proper procedures for the handling and sharing of data. The Minister's assurances that the Government has learned lessons, though welcome, are not sufficient to reassure us or, we suspect, the public. Access to NIR databases should be strictly limited and governed by clear protocols, which should be developed in consultation with the Information Commissioner. We recommend that the Home Office publish a detailed account of its plans for NIR access procedures.**

248. **The Home Office should address the Information Commissioner's concerns about the administrative information to be collected as part of the NIR. We accept that the Government's intention is to create an 'audit trail' to regulate access to NIR databases, but we are concerned about large stores of information about individuals' transactions and activities, particularly if registration is to become compulsory.**

249. **We recommend that the Home Office publish its plans for collecting and retaining administrative information as part of the NIR and that it commit to a principle of data minimisation for the National Identity Scheme. We seek assurance from the Home Office that it has taken full account of the potential of advanced privacy-enhancing technologies to reduce the amount of information it is necessary to collect in order to authenticate transactions and prevent fraud and unauthorised access.**

250. **We note that the Home Office has no plans to publish any specific privacy impact assessment of the National Identity Scheme. In terms of the design of the Scheme it is much too late for such an assessment to serve the intended purpose of integrating privacy considerations with the Government's plans to collect and store information. We recommend that on proposing any change in policy on the collection, storage, sharing or use of National Identity Register data, the Home Office make a report to Parliament on the implications of the change for an individual's privacy. The report**

246 Q 546

should address the following questions: how much extra information will be collected? For how long will it be stored? How many more people will have access to it? For what new purpose will it be used?

National DNA Database

251. The National DNA Database (NDNAD) is a publicly owned police intelligence database. It is governed by a Strategy Board chaired by ACPO with membership from the Home Office and the Association of Police Authorities. The Custodian of the NDNAD is accountable to the Board in ensuring, amongst other duties, that all profiles added to the NDNAD are reliable and compatible. The standards and procedures for the supplier laboratories are set by the Custodian.

252. Companies which analyse DNA samples and produce profiles for the NDNAD have to be accredited under the International Quality Standard for Testing Laboratories, ISO 17025. The companies store DNA samples and profiles on completion of analysis in case they need to be re-examined in the future and are required to store this material in a secure environment. The National Policing Improvement Agency (NPIA) has a "key role in maintaining and ensuring the integrity of the data entered and the use of the data in the investigation of crime".[247]

253. Section 64 of the Police and Criminal Evidence Act (PACE) provides that fingerprints, DNA profiles and samples taken in connection with the investigation of an offence may only be used for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution, or the identification of a deceased person or of the person from whom a body part came. The Act, including provisions on DNA profiles and samples, is currently under review.

254. Before 2001, the police could take DNA samples during investigations but had to destroy the samples and the records derived from them on the Database if the people concerned were acquitted or charges were not proceeded with. The law was changed in 2001 to remove this requirement, and changed again in 2004 so that DNA samples could be taken from anyone arrested for a recordable offence and detained in a police station. Once taken, DNA samples and profiles are normally retained indefinitely. The European Court of Human Rights (ECtHR) is currently considering a case (S and Marper v United Kingdom) in which the applicants have challenged the policy of retaining fingerprints and DNA from those acquitted or where no further action was taken. In a consultation exercise separate from that to be conducted on the PACE review, the Government will set out proposals on the retention of biometric data "in light of the ECtHR Judgment and comments received on this issue in response to the PACE Review process".[248]

255. The UK's database is the largest of any country: 5.2% of the UK population is on the database compared with 0.5% in the USA. During 2005–06, 715,239 new subject sample

247 Ev 265

248 Ev 272

records were added to the NDNAD, an increase of 37.25% on 2004–05.[249] On 31 December 2007, there were an estimated 4,264,251 individuals on the NDNAD.

256. A discrepancy between the number of DNA profiles and the number of individuals on the NDNAD has caused concern about the accuracy of information on the database.[250] A profile may be loaded on to the NDNAD on more than one occasion, creating "replicates". On 31 December 2007 there were an estimated 656,452 replicate profiles on the NDNAD: 13.3% of the total number of profiles. The NPIA told us that replication could occur "for example, if the same person provided different names, or different versions of their name, on separate arrests, or because profiles are upgraded".[251]

257. Meg Hillier MP told the House that replication rates were being reduced, "partly because in the early days of new DNA testing police forces took extra samples to meet higher evidential standards" and that "much work has gone on to educate police forces in taking DNA samples".[252] The NPIA's work to address the problem of replication includes the national implementation of Livescan, a system of automatic fingerprinting terminals located in police custody units.[253]

258. By the end of 2005, about 200,000 samples had been retained that would have been destroyed before the 2001 change in legislation. 8,000 of these samples matched with DNA taken from crime scenes, involving nearly 14,000 offences. These offences included 114 murders, 55 attempted murders, 116 rapes, 68 sexual offences, 119 aggravated burglaries and 127 offences of supplying controlled drugs.[254]

Assessing the benefits of the NDNAD

259. In 2005–06 45,000 crimes were matched against records on the DNA Database, including 422 homicides (murders and manslaughters) and 645 rapes.[255] In 2006–07 41,148 crimes were detected in which a DNA match was available or played a part and 452 homicides, 644 rapes and 222 other sexual offences were among the offences detected, the Home Office has said, "thanks to the help of DNA".[256]

260. The National Policing Improvement Agency (NPIA), which works in conjunction with the Home Office and the Association of Chief Police Officers on policy in relation to DNA, set out the benefits of the National DNA Database in terms of its contribution to the work of the police:

> The benefits of the NDNAD lie not only in detecting the guilty but in eliminating the innocent from inquiries, focusing the direction of inquiries resulting in savings in

249 National DNA Database Report for 2005–06, National DNA Database Strategy Board, September 2006

250 See for example "DNA database chaos with 500,000 false or misspelt entries", *Independent*, 26 August 2007

251 Ev 270

252 HC Deb, 21 April 2008, col 1032

253 Ev 265

254 Ev 272

255 http://www.homeoffice.gov.uk/science-research/using-science/dna-database/

256 HC Deb, 21 April 2008, Col 1032 (Meg Hillier MP, Parliamentary Under-Secretary of State, Home Office)

police time and in building public confidence that elusive offenders may be detected and brought to justice.[257]

261. According to the Home Office Forensic Science and Pathology Unit of the Home Office:

- the annual number of DNA detections more than doubled from 8,612 in 1999–2000 to 19,873 in 2004–05
- in 2004–05 a further 15,732 crimes were detected as a result of further investigations linked to the original case in which DNA was recovered
- on average the Database provides the police with around 3,000 matches a month
- DNA also helps by eliminating innocent persons from criminal investigations
- Serious offenders are often caught because they are arrested later for a relatively minor offence
- DNA helps to solve past crimes. A 'cold case review' programme has identified 215 serious offences dating back to 1989 for which DNA crime scene stains are available: 25% of these cases have been matched with an individual or another crime scene and 34 named suspects have been identified
- DNA scene-to-scene matches help identify patterns of criminal behaviour that may help solve past, existing and future crimes.[258]

262. Police witnesses and the Minister both highlighted the value of the NDNAD in solving 'cold cases' including, the Minister told us, "murders, rapes and the most serious of crimes." According to the Minister the NDNAD was the "root" of the solution of recent high-profile murder cases.[259] The NPIA highlighted the 21,199 'indirect detections'—crimes detected as a result of further investigation linked to the original offence—made in 2006–07, giving as an example of these circumstances those in which "an offender on being presented with DNA evidence of his involvement in an offence also confesses to other offences".[260]

263. Others who gave evidence to our inquiry, however, questioned the efficacy of the NDNAD in certain circumstances. Genewatch UK told us that its analysis of Home Office data shows that collecting more DNA from crime scenes has made a significant difference to the number of crimes solved, but keeping DNA from increasing numbers of individuals has not. Since April 2003, Genewatch UK told us in March 2007, about 1.5 million extra people had been added to the Database, but the chances of detecting a crime using DNA had remained roughly constant, at about 0.36%.[261] Genewatch UK acknowledged that "occasionally" the DNA of someone arrested for a minor offence is matched with DNA

257 Ev 265

258 Home Office, *DNA Expansion Programme 2000–2005: Reporting Achievement*, October 2005, pp 4 and 15

259 Q 498

260 Ev 272

261 Ev 182

from a serious past crime, "arguably justifying taking DNA from relatively large numbers of individuals". It did not accept, however, the assertion that the NDNAD provided an effective method of eliminating innocent people from police investigations:

> A DNA database is not required to provide evidence of guilt or innocence when there is a known group of suspects for a specific crime: a DNA profile can be obtained from each individual and compared directly with a crime scene profile. For the same reason, a database of individual DNA profiles is also unnecessary to exonerate an innocent person. The 'added value' of putting individuals on a database is only to introduce new suspects into an investigation.[262]

Weighing up the risks associated with collecting and retaining DNA

264. The Human Genetics Commission acknowledges the NDNAD "as a powerful criminal intelligence tool" but warns that its value could be undermined if the risks involved are not properly evaluated and public trust in the Government's intentions is undermined:

> there is a danger that its value in terms of crime detection and reduction could be used to justify the erosion of important freedoms, without prior analysis of the risks and benefits as to the likely good that may accrue from breaching privacy in the short term against the loss to society in the long term, as a result of citizens withdrawing their cooperation.[263]

265. Genewatch UK distinguished the collection and use of DNA from other forms of surveillance, pointing out the sensitive nature of the information DNA can yield and the consequences of its disclosure:

> DNA can … be used to investigate biological relationships between individuals (including paternity and non-paternity). A person's DNA also contains some other private information about their health and other physical characteristics. Some of this information (such as carrier status for a genetic disorder and non-paternity) may be highly sensitive and/or unknown to the individual.[264]

266. In its written evidence for our inquiry the Home Office sought to address concerns that the NDNAD could be used in an attempt to develop genetic profiles of those likely to offend. The DNA profile of an individual on the NDNAD, the Home Office told us, consists of a code number which represents the person's gender and ten markers from areas of DNA which do not play an active role in determining personal characteristics:

> The NDNAD therefore is not and will not be used in any attempt to correlate particular genetic characteristics with propensity to commit crime.[265]

262 Ev 180

263 Ev 204

264 Ev 180

265 Ev 193

267. Another risk to public confidence in the NDNAD is the perception that it could have a discriminatory effect in relation to particular groups. During our inquiry into *Young Black People and the Criminal Justice System* we heard from the then Minister Baroness Scotland that three-quarters of the young black male population would soon be on the DNA database:

> The implications of this development must be explored openly by the Government. It means that young black people who have committed no crime are far more likely to be on the database than young white people. It also means that young white criminals who have never been arrested are more likely to get away with crimes because they are not on the database. It is hard to see how either outcome can be justified on grounds of equity or of public confidence in the criminal justice system.[266]

268. Chief Constable Neyroud told us that the NPIA was "just finalising" work to assess the equality impact of the NDNAD, undertaken in response to the Committee's Report. He argued that addressing inequalities required examination of "the processes which finish with the DNA database" and the "whole system":

> The issue comes back to how people initially come into contact with the police, and the decisions that police officers make at street level about who and who not to [Stop and Search or arrest], not about the DNA database.[267]

Chief Constable Neyroud said that removing from the database records on individuals who were arrested but not subsequently charged would not reduce the overrepresentation of young black people on the NDNAD. In removing these records, he argued:

> all you do is take that total proportion of people off the database; you do not affect the overall equality of the database itself.[268]

Debate on the scope of the NDNAD

269. One of the most controversial aspects of the debate on the National DNA Database is the issue of the retention of the DNA of individuals who have been arrested but not subsequently charged with an offence. Noting the over-representation on the database of Afro Caribbean males and the retention of the DNA of "thousands of young people under 16 with no criminal conviction or caution", Liberty accepted that there was "a need for a limited database of those convicted for certain offences (generally involving violence or sexual assault)" but that DNA was "irrelevant in most criminal cases and the vast majority of entries on the register will be of no use in solving crimes".[269]

270. Genewatch UK called for "a return to taking DNA on charge rather than arrest, except where it is needed to investigate a specific offence" and a system of time limits on how long

266 Home Affairs Committee, Second Report of Session 2006–07, *Young Black People and the Criminal Justice System*, HC 181, paragraph 33

267 Qq 483–84 (Chief Constable Neyroud)

268 Q 485 (Chief Constable Neyroud)

269 Ev 190

Database records are retained "so that only DNA profiles from people convicted of serious violent or sexual offences are kept permanently".[270]

271. Police witnesses and the Minister disagreed with such proposals. Chief Constable Neyroud told us that:

> Many of the 450-odd murders that DNA contributed to [solving] have arisen from relatively minor offences—theft, … driving offences of that nature, that have been committed by offenders either before or after.[271]

In his response the Minister referred to:

> the cold cases and others that we have since solved—murders, rapes and the most serious of crimes—by having someone's DNA … perchance on the database when originally it was only on the database because of very minor offences.[272]

272. We also asked our witnesses about suggestions that the NDNAD should be expanded in terms of the number of samples collected and the functions of the database. Chief Constable Neyroud said that in relation to a reported suggestion that the NDNAD should include samples from children who exhibit certain behaviour indicating future criminal activity, "there is a level of knowledge and detail now about criminal career history, which would indicate that there are some people who are more likely to offend". He stated:

> There would be no way that I would suggest we move ahead in any of that direction without the Independent Ethics Committee and, indeed, some of the recommendations out of the Nuffield Report in this territory informing that debate.[273]

273. Dr Eric Metcalfe of JUSTICE argued that the limits on the use of DNA *samples* taken for the Database were so broadly drawn that researchers could seek to explore links between genetic characteristics and criminal behaviour:

> Obviously the police DNA database has its own regulatory framework and there are high ethical standards in relation to medical research, but I am not going to say it is impossible. I know that medical searches have already been approved in relation to it.[274]

The NPIA pointed out that DNA *profiles* are sequences of numbers obtained by analysing parts of samples which "do not contain genetic information".[275]

274. The Minister rejected suggestions that inclusion on the NDNAD carried implications of criminality:

---

270 Ev 179

271 Q 476 (Chief Constable Neyroud)

272 Q 498

273 Q 469 (Chief Constable Neyroud); Nuffield Council on Bioethics, *The forensic use of bioinformation: ethical issues*, September 2007

274 Q 286 (Dr Metcalfe)

275 Ev 271

> we will look at retention criteria and other matters very seriously, but I do not accept the starting premise that somehow this informational and investigatory tool is counter civil liberties because it is not a database that is about the guilty, or, in the State's terms, the potentially guilty, that is why they are on. That is not the case at all.[276]

275. The Minister told us that "broadly where we are now, notwithstanding the PACE review, is where we should be … we are roughly in a reasonable place in public policy and civil liberties terms given the nature of the database". He was "not convinced" by the notion of a 'universal' DNA database and "fairly agnostic" about proposals that samples should be taken from those suspected of non-recordable offences, although he "would probably lean towards not doing so rather than otherwise."[277]

Maintaining confidence in the database: practical considerations

276. In giving evidence on the idea of expanding the NDNAD Chief Constable Neyroud stressed the need for transparency in relation to the functions and administration of the database:

> I think the most important thing with the DNA database is being really clear with the public what the purpose of the database is, what its effectiveness is, how well it is being managed and the custodianship of it, how well and independently the research processes are being done, so that the public can continue to have confidence in the way in which biometric data is being managed.[278]

Chief Constable Neyroud set out how individuals (such as victims and witnesses) who gave samples on a voluntary basis negotiated "two layers" in consenting to the collection of their DNA, choosing either to have it matched against the database for the purpose of a specific crime, or to have it added to the database.

277. The NPIA has worked to improve the information it provides about the NDNAD. According to Chief Constable Neyroud:

> much clearer leaflets … will be available to people so that the consent is not just informed but people are clear about what they have signed up to and what the process is.[279]

Chief Constable Neyroud said that "the majority of people" seemed "quite relaxed to have their data on the database":

> Relaxed as in they have had it explained to them that the database is not a surveillance database, it is an intelligence database that will only match you to DNA

276 Q 501

277 Qq 488, 501

278 Q 469 (Chief Constable Neyroud)

279 Q 471 (Chief Constable Neyroud)

> if it comes out of a crime scene … and most people seem quite happy, in those circumstances, to provide their data to the database on a voluntary basis.[280]

278. Several Members of Parliament have made representations on behalf of constituents who wish to have their DNA removed from the National DNA Database.[281] When we challenged Chief Constable Neyroud about the concerns of those who wished DNA samples taken from them to be destroyed he said:

> There is a small group of people who are very concerned about it, not least of which we have not, in my view, explained effectively what the linkage is, for example, or the non-linkage, between DNA and vetting and that connection. There is not a connection.[282]

The Minister's view was that:

> If we are coming up with a much clearer retention policy, a much clearer criteria for retention, and a much clearer process for the general public should they want to come off the database and to at least have that avenue explored, I think that would be better all round and go to supporting the integrity of the DNA database.[283]

Whilst Mr McNulty hoped that the review of the Police and Criminal Evidence Act would achieve these aims he had earlier noted that:

> others, and it may be an area we should look at, my mind is not settled on the matter, are less than happy that PACE is really the statutory core of the existence of the DNA database rather than more formally put on primary legislation.[284]

279. LGC Laboratories Ltd, one of the two main suppliers of expert forensic services to law enforcement agencies, supported the system of oversight of the NDNAD, deeming it to be "extremely effective". It also identified, however, several issues concerning:

> the transfer and security of data and samples where we think that appropriate design of future systems could minimise the potential risk of inappropriate access to or use of information.[285]

LGC argued that the laboratories do not need all of the data about the donor which is provided to them in order to be able to process the samples and rectify errors, and raised questions about retention of the data:

> In practice, it is accepted that any system involving large-scale sample and data collection and transfer can be prone to error, such as occasional inadvertent 'sample swaps', so some additional data is of value in case it is necessary to resolve a

280 Q 473 (Chief Constable Neyroud)

281 On 15 October 2007, for example, Mr Stephen Crabb raised this issue during Home Office questions: HC Deb, Cols 544–545

282 Q 474 (Chief Constable Neyroud)

283 Q 499

284 Q 497

285 Ev 162

> discrepancy. However, this could be limited to a less specific identifier than a donor's name, for example a date of birth.
>
> The residual samples are retained in case rework is required, including reprocessing for quality assurance. The ability to re-profile samples is of undisputed value, but storage of samples, containing the full DNA of donors, has raised issues of security, access and approval for use.[286]

280. Genewatch UK also queried the need to retain DNA samples. It noted that in some other countries—such as Germany—individuals' samples are destroyed once the DNA profiles used for identification purposes have been obtained, and argued that:

> Only temporary, not permanent, storage is necessary for quality assurance purposes and a new sample can always be taken from the suspect if a DNA profile requires checking or upgrading.[287]

281. **We recognise the National DNA Database as a valuable investigative tool, particularly in relation to police efforts to solve older cases. But the sensitive nature of the information which may be yielded by DNA heightens the degree of responsibility borne by the Government. The Home Office must work with the National Policing Improvement Agency and the police to set and observe a regulatory framework which protects individuals from unnecessary invasions of privacy and loss or unauthorised use of their genetic material and information gleaned from it.**

282. **The Home Office should actively support the NPIA in its efforts to reduce the rate of replication on the NDNAD. Inaccuracies in the information on the database must be corrected to enable the police and the public to reap the full benefit of the NDNAD.**

283. **We welcome the Government's assurance that the National DNA Database will not be used in any attempt to correlate particular genetic characteristics with propensity to commit crime. We recommend that the Home Office renew this assurance in conjunction with the Government's conclusions on the review of the Police and Criminal Evidence Act. We recommend that the Home Office make public at the earliest stage any plans to revisit this issue.**

284. **The Government's consultations should help to clarify the purposes and processes of DNA collection and retention. We endorse the views of the NPIA and the Minister that these purposes and processes must be transparent in order to maintain confidence in the database as a proportionate response to crime.**

285. **There have been calls for an expansion of the National DNA Database to include profiles connected with non-recordable offences and for a 'universal database' and for the Government to reconsider its policy on retaining the profiles of those who have been arrested but not charged. In order to facilitate a full debate and an appropriate level of Parliamentary scrutiny we recommend that alongside any conclusions of the PACE review the Government introduce primary legislation to replace the current**

286 Ev 163

287 Ev 182

regulatory framework for the National DNA Database. We recommend that this legislation provide for a more accessible mechanism by which individuals can challenge the decision to retain their records on the Database.

286. **The Government should reconsider the ways in which National DNA database information is collected, handled, stored and transferred. In particular we recommend that in order to minimise the data held, the Home Office and the police should review the identifiers used for samples and the policy of retaining samples.**

The potential of other public and private sector databases for use in the fight against crime

287. The Data Protection Act contains exemptions relating to law enforcement and national security, which remove the obligation on data controllers to observe all the rights normally afforded individuals in respect of their personal information. Data controllers may disclose information for the purposes of prevention and detection of crime and the apprehension or prosecution of offenders.

288. During our inquiry the Information Commissioner's Office stressed that in these circumstances protecting privacy and individual liberty remained important. The Deputy Information Commissioner, David Smith, also called for the relative severity of different crimes to be assessed when contemplating any collection or use of personal information which might impinge on privacy:

> Terrorism is, if you like, the highest in the scale, but there is still a question, even with terrorism, as to how far you go in intruding into the private lives of everybody in the country in order to fight against terrorism. In everything there is a question of proportionality. A greater degree of intrusion is proportionate in fighting terrorism than is proportionate in fighting shoplifting.[288]

The Information Commissioner told us that "sometimes, when the threats are the greatest, the need for safeguards is the strongest". He added:

> Yes, the fight against terrorism is paramount, but, even there, there has to be some framework to make sure the authorities do not overstep the mark.[289]

Information-sharing and data-matching

Access by public agencies to private databases

289. The potential of private databases in respect of the fight against crime raises new challenges for governments in balancing the right to individual privacy with the need to protect the public. The Royal Academy of Engineering argued that if individuals consent to their data being recorded on a database for a given purpose, that data should not be used for purposes for which consent has not been given; in general, "public agencies should not be allowed access to private databases". The need to investigate crime could provide a

288 Q 31 (David Smith)

289 Q 31 (Richard Thomas)

justification for permitting access to such databases but, the Royal Academy of Engineering argued, "there must be good reason for allowing that access, in the form of significant reason for suspicion of fraud or other financial crime".[290]

290. We asked the Information Commissioner's Office about the potential use of information from private sector databases, such as those used to manage loyalty schemes. The Deputy Information Commissioner told us that the police had accessed store card information in the course of investigations. He said that "narrowing down what you need" was the appropriate course to take, as opposed to speculative access to "lifestyle information" which would amount to "fishing".[291]

The Serious Crime Act

291. The Audit Commission's National Fraud Initiative (NFI) is a data-matching exercise carried out every two years as part of the statutory audit of local authorities and NHS bodies (under the Audit Commission Act 1998). The NFI matches datasets including the audited body's payroll, student awards and loans, housing benefits, housing rents, the blue badge parking scheme for the disabled and single person council tax discounts to identify possible anomalies that could indicate fraud or erroneous overpayment.[292]

292. The Serious Crime Act provides a legislative gateway for public authorities to share information for the purpose of preventing fraud through a designated anti-fraud organisation. It creates a route by which public and private sector bodies can contribute their data to the Audit Commission for the purposes of undertaking data-matching in order to prevent or detect fraud. It also makes the contribution of data for such purposes mandatory for some bodies (in particular local government and NHS bodies). This measure, the Commission told us, would "enable government departments and agencies to use the NFI as a conduit for data sharing to address local and national fraud risks in a controlled, secure and well regulated environment".[293]

293. During the passage of the Bill the Information Commissioner highlighted the importance of limiting access to data and information-sharing powers:

> We need a framework to make sure that the legitimate purposes of the police and the law enforcement bodies are served by accessing this data, but it is not a free-for-all; they cannot just go in and look at everyone's data and just make merry with it; it has to be targeted, proportionate, for a defined purpose.[294]

Liberty also raised concerns about the Bill's proposals to extend the Audit Commission's power to "mine data in order to identify potential fraudsters".[295]

290 Ev 164

291 Qq 53–54

292 Ev 132

293 Ev 133

294 Q 21 (Richard Thomas)

295 Q 284 (Mr Russell)

294. The Ministry of Justice told us that it had worked with the Home Office and the Information Commissioner to ensure that provision for information-sharing to prevent fraud matched the demands of putting in place "sophisticated" arrangements and "complex" protections:

> There was a lot of discussion between the two departments and with the Information Commissioner on exactly what was the best way of achieving the policy objective. As the legislation went through Parliament there were a number of changes made, particularly the introduction of the requirement for a Code of Practice. It is a good example of spotting the issue, working together between departments and with the Information Commissioner to find the best way of addressing that issue, making sure that we have the right powers in place to do it and also listening to the views of Parliament and being prepared to make amendments as the legislation goes through.[296]

Transport databases

295. We heard evidence on police use of transport data, such as images captured by camera surveillance, for the purposes of crime detection. Steve Burton from Transport for London told us that in total TfL received 300–350 requests a month for data including information captured on the Oyster system, relating to individual journeys. In comparison with the three and a half billion journeys taken on the TfL network every year, Mr Burton told us, this was "a fairly small number of requests".[297]

296. The Department for Transport told us that automated number plate recognition (ANPR) cameras used by the Highways Agency for traffic flow control "would not help the Police" because vehicles passing the ANPR camera sites could not be accurately identified or cross-referenced against other databases.[298]

297. Chief Constable Neyroud of the National Policing Improvement Agency (NPIA) argued that in order to secure benefits from the sharing of bulk ANPR data the police's efforts had to be properly focused:

> You will throw up an awful lot of matches otherwise, without the ability to resource it … It is not just about joining up the data, we have to join up the back office techniques that mean that we are focused and effective and we are picking the right targets. The work that we have done in that territory around, for example, the Birmingham ring-road with the combined motorway patrol group there linking the ANPR shows that we can be many times more effective with that type of data, we can be getting very high levels of hit rate as vehicles go out, but, of course, if you have to follow through into the offences brought to justice, we, the NPIA also have to streamline the paperwork for summary cases, the back office support, the case and

296 Q 403 (Clare Moriarty)

297 Qq 383–4 (Steve Burton)

298 Q 367 (Dr Stephen Hickey)

> custody system, so that we are not dragging police officers off the street as we get more hits.[299]

The Minister told us that ANPR had proved "very useful, not least in terms of serious crime and some particular terrorist cases" and that he was keen for the law in respect of sharing ANPR data to be "in a far more settled position than it is now".[300]

Profiling to predict criminal behaviour: patient data and children's databases

298. The Information Commissioner has sought to raise awareness of the exploration and use of profiling techniques developed in the private sector—which help companies to predict customers' preferences and target their marketing—by public agencies. The Commissioner warned that automatic compiling and searching across databases to detect patterns of behaviour and predict future behaviour could "build up images of people which may take you in the wrong direction":

> If you are trying to identify children who will commit crimes later in life—I understand that the Cabinet Office is doing a lot in this sort of area—I understand their motivations and I understand what they are trying to achieve, but if they get it wrong—if they label that youngster as someone who is going to be a criminal in 10 or 15 or 20 years' time or that family as a problem family—it needs our intervention. Technology can take you a long way but it is not going to be 100% effective. When we raised concerns about profiling we raised concerns about social sorting. It is to signal the risks involved without the human intervention. Machines can do a lot to gather and to help you inform your decisions but without the human intervention I think there are grave dangers.[301]

299. The Commissioner did not suggest a ban on profiling by the public sector but urged the Government to proceed with caution:

> if public bodies embrace the potential of the technology too literally and too enthusiastically it will undoubtedly create the sort of climate of suspicion, lack of trust and real problems. It will only take a handful of star examples which get splashed over the newspapers to destroy all the good work that the health authority, the social services, the education [services] and all the other people are trying to do to use information intelligently.[302]

300. Dr Ian Forbes argued that predictive profiling effected a shift from monitoring a person's potentially criminal behaviour to labelling that person a criminal:

299 Q 459 (Chief Constable Neyroud)

300 Q 507

301 Q 76 (Richard Thomas)

302 *Ibid.*

> They are scanned through your profiling system and then they are labelled … They are then treated as if they are equivalent to that label. It is just as lazy as stereotyping.[303]

We asked Dr Forbes about the potential of profiling in terms of helping the police to concentrate their efforts. In response Dr Forbes set out the risks posed by this approach:

> past experience shows that the targeting of the efforts often runs out to be discriminatory in practice on the ground, so that its use is complicated. It may well be that there was more crime amongst a certain group but why is that? It may be because that group is already targeted and more crimes were picked up.[304]

301. Professor Simon Wessely also told us—in responding to a suggestion that patient information might be used to profile people whose behaviour might threaten the public—that predictive profiling was dangerous. Any action taken on the basis of such profiling might well be based on incorrect assumptions and would therefore represent a disproportionate response in relation to the risks associated with not taking action:

> The problem is that it is incredibly inaccurate. It is okay for a large group of people and so you can make predictions about large samples in populations, but when it comes to the individual, it is incredibly inaccurate. The risk of hazard and detriment to that individual being deprived of their liberty for things that they are not going to do is very high as opposed to the one person who is going to commit a serious offence.[305]

Professor Wessely also pointed out that use of sensitive patient records in this way would be "destructive" to the care of patients and management of health services. He told us that any such development would "just be quite an appalling future".[306]

302. Professor Carol Dezateux said that whilst the development of an index of children for child protection purposes constituted an "advance", attempting to use such a database to predict criminal activity would be risky for the same reasons:

> just because certain factors are associated with an increased likelihood of a behaviour, it does not mean that just because they are present in an individual that they are behaving in this way.[307]

Home Office perspective on information-sharing and the fight against crime

303. Taking into account the disappearance of technological and cost barriers to sharing information and searching across databases, we asked the Minister whether or not the

303 Q 272 (Dr Forbes)

304 Q 274 (Dr Forbes)

305 Q 275 (Professor Wessely)

306 Q 276 (Professor Wessely)

307 Q 276 (Professor Dezateux)

Home Office was in favour of the convergence of the stores of information held by Government. Mr McNulty responded:

> For some of the more substantial databases it is appropriate that they are shared across government more and more, and in the light of the reviews and everything else that we are undertaking we can be very clear on the civil liberty side as well as data protection, data security and others.[308]

304. On being pressed about a Home Office interest in health-related or children's databases the Minister rejected the idea that the Government wanted to "go fishing every time there is a database":

> If you go back to the example of ANPR, where that is used in an investigative fashion, it is around very strict search criteria and is not going fishing just for the sake of it. I do not think there is any efficient way or policy that would dictate the Government just want to go fishing because we are nosy into assorted databases or the product of other data streams.[309]

Mr McNulty did not accept suggestions that the DNA database be expanded to include records for primary school children deemed likely to display criminal behaviour in future:

> We are then getting into the realms of … the sort of potentially guilty or the future guilty, and I do not accept that at all.[310]

305. **In its use of databases and other means of collecting, storing and using personal information the Home Office should explicitly address these questions: in the context of the fight against crime where should the balance between protecting the public and preserving individual liberty lie? How should this balance shift according to the seriousness of the crime? What impact will this have on the individual and on our society as a whole?**

306. **Even as society confronts its most serious threats it must protect its liberties. The fight against crime in general does not provide sufficient justification for information-sharing which might have an impact on privacy. It is vital that before information is shared for purposes other than those for which it has been collected those purposes are subjected to the closest scrutiny.**

307. **Information-sharing must only be carried out in the context of a robust statutory framework which incorporates tests of proportionality and mandates the securing of consent where possible. The effectiveness of information-sharing should be assessed at the stage at which a new project is proposed, in order to prevent unnecessary sharing and retention of data. We recommend that where the sharing or matching of information held by the Home Office or its agencies is proposed, the Information Commissioner should act as a consultee and mediator on the same footing as the Ministry of Justice.**

308 Q 495

309 *Ibid.*

310 Q 503

308. **Exemptions from the Data Protection Act notwithstanding, in giving consent and choosing services individuals are better informed about how their information is used and shared in the private sector than they are about how it might be used and shared by the Government. We recommend that the Home Office work with the Information Commissioner to raise awareness of how information generated in the private sector—such as details of retail purchases, or information posted on blogs or social networking sites, for example—might be used in the investigation of crime.**

309. **We welcome the Minister's reassurance that the Government is not interested in "fishing" for information about individuals. However, we do not underestimate the lure of new technological capabilities and new ways of sharing and matching information from a range of sources, which might appear to offer benefits in the fight against crime. The Home Office should exercise a 'self-denying ordinance' in relation to its use of technological capabilities and its power to collect personal information.**

310. **We would be particularly concerned by any attempt to use patient data or information held on children for the purposes of predictive profiling for future criminal behaviour rather than child protection: the Home Office must not undertake or sponsor work of this sort.**

Regulation of Investigatory Powers Act

311. In our inquiry we have focused on the growth in potential for surveillance—and the associated benefits and risks—which has come about as a result of an increase in the collection of personal information in databases, rather than on the directed and covert surveillance carried out by the police and security services. However, we did take evidence on some aspects of this work—predominantly authorisation and oversight and the recent increase in requests for communications data—and we took the opportunity offered by this inquiry to question police and Home Office witnesses on the implications of Sir Christopher Rose's report on the covert recording of conversations at HM Prison Woodhill.

312. The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative framework for the use of methods of surveillance and information-gathering used in efforts to prevent crime, including terrorism. RIPA makes provision for:

- The interception of communications
- The acquisition and disclosure of data relating to communications
- The carrying out of surveillance
- The use of covert human intelligence sources
- Access to electronic data protected by encryption or passwords

- The appointment of Commissioners and the establishment of a tribunal with jurisdiction to oversee these issues.[311]

313. In a report for the period 1 January 2005 to 31 March 2006 the then Interception of Communications Commissioner, Sir Swinton Thomas, noted that since he had taken up his post in April 2000 the number of organisations that he was required to inspect and oversee had grown. At the request of the Home Secretary he had undertaken the inspection of interception in prisons, and on 5 January 2004 Chapter II of Part I of RIPA had come into force, enabling named organisations approved by Parliament to acquire communications data (the records—but not the contents—of communications traffic such as mobile phone calls and emails). At the date of his report the organisations that the Interception of Communications Commissioner was required to inspect and oversee—795 in all—were as follows:

- The nine Agencies empowered lawfully to intercept communications under section 6 of RIPA
- 52 police forces
- 12 other Law Enforcement Agencies such as the Royal Military Police and the British Transport Police
- 139 prisons
- 475 local authorities authorised to acquire communications data
- 108 other organisations, such as the Financial Services Authority, the Serious Fraud Office, the Independent Police Complaints Commission, the Ambulance Service and the Fire Service who are authorised to acquire communications data.[312]

314. RIPA powers are used by a wide range of public authorities which have:

> necessary and proportionate requirements to engage in conduct that can interfere with individuals' rights for legitimate purposes whether to safeguard national security or to prevent and detect crime.[313]

315. Oversight is carried out by the Chief Surveillance Commissioner, the Interception of Communications Commissioner and the Intelligence Services Commissioner.

Authorisation and oversight of RIPA powers

316. The Home Office outlines the system of oversight in place for RIPA:

> Conduct [under the Act] may be undertaken only when necessary for a legitimate aim and proportionate to that aim and is subject to strict independent oversight by the Chief Surveillance Commissioner, by the Interception of Communications

311 Home Office, *Security: Regulation of Investigatory Powers Act*. Available at: http://security.homeoffice.gov.uk/ripa/

312 *Report of the Interception Communications Commissioner for 2005–06*, HC (2006–07) 315, p 3

313 Ev 194

> Commissioner and the Intelligence Services Commissioner—all of whom report to the Prime Minister and to Parliament. RIPA also provides access for complainants to an independent tribunal—the Investigatory Powers Tribunal.[314]

317. Liberty argued that "the scope of those able to use RIPA powers is wide with a huge range of public bodies having access to them" and that:

> 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.[315]

In a case which has received a great deal of attention in the media, Poole Borough Council used powers under RIPA to establish whether or not a family had lied about living in a particular school catchment area. The family's movements to and from school were tracked, satisfying the Council that the family's application for a school admission was valid. The mother of the family was reported to have regarded the incident as "a huge infringement" of her liberty and to have said that her daughter was now afraid of "a man outside watching us". The Council's action was been criticised by Liberty as disproportionate and intrusive; the Home Office's reported response was that RIPA legislation did not appear to have been used inappropriately.[316]

318. Liberty drew a distinction between the operation of RIPA and the US surveillance process which requires a warrant from a court for surveillance of a US citizen. The use of "National Security Letters"—rather than warrants issued by a special Foreign Intelligence and Surveillance court—to intercept communications to the US, has been deemed unconstitutional by the US Federal Court.[317]

319. JUSTICE also drew international comparisons, stating that the UK was "virtually alone" among common law countries in allowing the interception of telephone calls, emails, letters and faxes by authorisation of the Home Secretary rather than by a judge:

> In our view, the power of the Home Secretary to issue interception warrants for both intelligence and law enforcement purposes should be replaced with a scheme for judicial authorisation of interceptions. This would bring the UK into line with the practice of virtually every other common law country.[318]

JUSTICE compared the "detailed, open and transparent reports" produced by the Canadian and United States federal governments on the use of electronic surveillance with the "paucity of information" made available by means of the published reports of the UK Interception of Communications Commissioner.[319]

---

314 Ev 194

315 Ev 190

316 "Council uses criminal law to spy on school place applicants", *Guardian*, 11 April 2008

317 Ev 190

318 Ev 214

319 Ev 213

320. The Association of Chief Police Officers (ACPO) worked with the Home Office on a joint review of RIPA, which reported in 2006. ACPO emphasised the importance of RIPA powers in the investigation and prosecution of serious crime, and in enabling the police to take swift action in an emergency. It argued, however, that:

> the regime that has developed around RIPA has become unnecessarily bureaucratic and has been characterised by a risk-averse approach that has proved wasteful and has hampered investigations.[320]

321. ACPO has also called on the Government to explore the establishment of a single Commissioner for activities governed by RIPA. It also argues that whilst the police are required to "have a high level of authority" before accumulating data about individual's private life, private sector organisations "appear to be able to do so with impunity".[321]

322. Assistant Chief Constable Gargan, representing ACPO, told us that whilst a risk-approach requiring detailed risk assessments and authorisations had its place "when you are dealing with techniques that really do risk infringing on people's liberties"—such as covert investigative techniques, powers under the Police Act, intrusive surveillance under RIPA and long-term directed surveillance—there was a case for reassessment where:

> we are effectively dressing up routine law enforcement activity as covert surveillance and over-authorising in those circumstances.[322]

Assistant Chief Constable Gargan gave as examples of such activity turning a CCTV camera to focus on a parade of shops or offering the victim of racist graffiti a camera in his or her home to film people offending.[323] Whether or not the adjustment of surveillance cameras in this way required authorisation under RIPA was "a moot point".[324]

323. Since the report of the RIPA review was published, ACPO has referred to the Home Office those issues—relating to bureaucracy—on which ACPO and the Surveillance Commissioners could not agree.[325] These included a number of scenarios on which ACPO's view was that authorisation should be the exception rather than the rule.

Communications data

324. The Minister stressed the distinction between interception of the contents of an individual's telephone calls and emails and access to communications data: "just the traffic; not the content". Mr McNulty accused the media of "quite deliberately" conflating the two:

320 Ev 214

321 Ev 217

322 Q 418 (Assistant Chief Constable Gargan)

323 Q 416 (Assistant Chief Constable Gargan)

324 Q 419 (Assistant Chief Constable Gargan)

325 Evidence taken by the House of Lords Constitution Committee on 16 January 2008, Qq 128–9

> You will have all seen press coverage saying seven or eight hundred authorities all bugging your phone and looking at your emails and everything else, which is completely wrong—and quite rightly wrong.[326]

325. We asked the Minister about levels of public awareness of the wide powers granted by RIPA to permit access to communications data. Mr McNulty said that "The more people are aware the better, and they can always be more aware than they are" and went on to assert that "if people are involved in entirely legitimate activities then they do not have to worry about RIPA at all".[327] The Minister defended the right of local authorities to request that communications data be collected in order to tackle crimes in their areas:

> If someone with a significant track record for fly-tipping or whatever else in a local area persists and the local authority under its statutory duty wants to see if he has been phoning the fella on the other side of town who is in the middle of a construction site and no one knows where his rubbish is going, that is perfectly legitimate.[328]

Report by Sir Christopher Rose on the HMP Woodhill case: the Wilson Doctrine

326. On 4 February 2008 the Secretary of State for Justice told the House that he had asked the Chief Surveillance Commissioner, Sir Christopher Rose, to investigate the circumstances relating to visits to a prisoner—Babar Ahmad—at HMP Woodhill in May 2005 and June 2006, to establish whether the visits were subject to any form of surveillance and if so by whose authority and with whose knowledge.[329] Sir Christopher's report was laid before the House on 21 February. He found that the monitoring had been carried out lawfully under the legislation and that it was properly authorised and fully documented.

327. Sir Christopher noted that the surveillance he had been asked to investigate did not appear to him to be within the scope of the Wilson doctrine, which relates to the tapping of Members' telephones and applies to all forms of interception subject to authorisation by the Secretary of State: monitoring of conversations at HMP Woodhill is not interception as defined by the legislation and did not require such authorisation.[330]

328. At the end of his report, Sir Christopher said that there was "manifest scope for confusion in the minds of officers of public authorities and MPs as to the correct inter-relationship between the Wilson doctrine and the legislation" and that he believed that

326 Q 514

327 We note the concerns raised by the Information Commissioner's Office in response to media reports that the Government intends to amend RIPA to provide for a centralised database of communications data which would contain details of every telephone call, email and internet site visited by members of the public. See, for example, "'Big Brother' database for phones and emails", *Times*, 20 May 2008

328 Q 518

329 HC Deb, 4 February 2008, cols 660–661

330 *Report on two visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill: report of an investigation by the Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner*, Cm 7336, February 2008, p 2

"clarification of this inter-relationship would be welcomed by everyone".[331] In her statement on Sir Christopher's Report, the Home Secretary told the House that:

> the Government will review the statutory codes of practice, and in particular … we intend to clarify that, as regards covert surveillance, conversations between Members of Parliament doing their constituency business and their constituents should be considered as "confidential information", and treated in the same way as other confidential information, such as conversations between a person and their lawyer or minister of religion. That will more clearly give such conversations additional protection.[332]

329. Assistant Chief Constable Gargan told us that very few "ACPO colleagues" were aware of the Wilson doctrine at the time of the initial media coverage of the recording of the conversations in question. He made four points in response to Sir Christopher Rose's report:

- it was helpful to clarify that the Wilson doctrine applied only to those covert activities requiring ministerial authorisation and not to property interference and intrusive surveillance, when carried out by police forces
- ACPO believed that adequate provision existed within RIPA to ensure that an individual's privacy was respected and that "considerations of necessity, justification, proportionality, collateral intrusion, et cetera" were taken into account when authorisations were made
- ACPO broadly supported the suggestion made by the then Interception Commissioner in 2006 that the Wilson doctrine should be abolished and if necessary provided for in legislation or in a code of practice
- the discussion had uncovered a "technical defect" in RIPA in that it made no mention of confidential information: this served to strengthen the case for a revisiting of the legislation and a revision of the Act.[333]

330. When we asked the Minister to indicate the lessons learned by the Government from the incident he told us that in looking at "all the assorted statutory codes of practice that prevail around the whole issue of surveillance and intercept, not least in the context of Wilson":

> we should get to a stage where confidential discussions between an MP and his or her constituents in the broadest sense should be as sacrosanct as a legal discussion between an appointed legal representative and an individual.[334]

The Home Office intends to publish draft codes of practice for consultation over the summer of 2008 and to lay revised codes before Parliament in the autumn.[335]

---

331 *Report on two visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill: report of an investigation by the Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner*, Cm 7336, February 2008, pp13–14

332 HC Deb, 21 February 2008, col 538

333 Qq 428–30 (Assistant Chief Constable Gargan)

334 Q 525

331. **We recognise the distinction drawn by the Minister between the degrees of intrusion caused by the interception of communications and access to communications data. In our view, however, access to communications data by a relevant authority has a significant impact on an individual's privacy. We note the increase in requests for access to communications data in recent years and the large number of organisations empowered by RIPA to make such requests. Whilst communications traffic continues to increase and diversify, the provisions of RIPA in respect of communications data are not well understood. We recommend that the Home Office use the opportunity afforded by the latest review of RIPA codes of practice to take steps to raise public awareness of how and why communications data might be collected and used.**

332. **For each new organisation authorised under RIPA to request access to communications data, the Home Office should produce a statement setting out the purposes for which the data will be used and evidence that access to communications data represents a proportionate response in terms of the problem to be addressed and the impact on individual privacy. Any assessment carried out by the Home Office should apply a test of proportionality: a potential intrusion which might be justified by the need to investigate terrorism would not be justified by efforts to tackle minor crimes such as littering.**

333. **We note in the context of debate on the application of RIPA authorisations, the range of views on whether or not actions such as adjusting CCTV cameras constitute surveillance as defined by the Act. We also have serious concerns about the deployment of surveillance in relation to less serious crimes, which have been raised by—amongst other things—the use of RIPA powers to establish the validity of an application for admission to a school. The Home Office should undertake a public consultation on the levels of authorisation which should be required for various surveillance activities and the purposes which would justify different levels of intrusion.**

334. **We are concerned by the implications for Members of Parliament of the events investigated by Sir Christopher Rose. Constituents must be able to speak freely to their Members of Parliament without fear of intrusion by the state. We reserve the right to return to this issue in due course.**

Conclusions and recommendations

Introduction

1. We reject crude characterisations of our society as a surveillance society in which all collections and means of collecting information about citizens are networked and centralised in the service of the state. Yet the potential for surveillance of citizens in public spaces and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the Government's intentions in relation to data and data sharing is preserved. The Home Office in particular and Government in general must take every possible step to maintain and build on this trust: our Report provides a starting point. (Paragraph 14)

Surveillance in context

2. Advances in technology have supported a significant increase in the potential for surveillance of the activities of individuals in the United Kingdom. We welcome the Information Commissioner's efforts to raise awareness of this trend, particularly in relation to the collection of personal data, and to encourage the Government to consider the implications of the growth of surveillance for the individual and society. We recommend that the Information Commissioner lay before Parliament an annual report on surveillance, and that the Government produce a response to each report, also to be laid before Parliament. We further recommend that Parliament have the opportunity to hold an annual debate on this issue. (Paragraph 36)

Why has the use of surveillance increased?

3. Technological advances in terms of the collection, storage and use of personal information have enabled the private sector to target its communications at particular groups of consumers and to provide more personalised services. The development of this capability has produced an increasing reliance on digitally-supported means of making decisions. We do not dispute the benefits to the consumer of an impartial decision-making process on the one hand and a more appropriate and convenient service on the other. We do, however, note that these benefits depend on the accuracy of the data collected and the security of the systems in which the data is held. (Paragraph 52)

4. A strong common theme is emerging in both the private and public sector: a move towards more personalised services which require the service provider to collect information from individuals in order for the service to be effective. Whilst the outcome may be more personalised, however, the trend in terms of input is a standardisation of the information requested with a tendency to collect information which may identify an individual even where this is not needed in order to provide or improve services. (Paragraph 76)

5. We recognise the desire of private and public sector service providers to make full use of the opportunities provided by technology in relation to targeting and facilitating access to services and products. We also accept that advances in

technology have heightened the public's expectations of what technology can deliver not only in terms of convenience but also in connection with the prevention and investigation of crime. The elimination of technological barriers to the collection, storage and sharing of large volumes of information, however, has significant implications for individual privacy and potentially for society at large. (Paragraph 77)

6. The Government should be open about its intentions in relation to collecting personal information, and should make sufficient time for public and Parliamentary debate on its proposals. In general the Government should move to curb the drive to collect more personal information and establish larger databases. (Paragraph 78)

What are the implications of the growth in surveillance for the individual and society?

7. The technological developments which facilitate the collection, storage and use of information about individuals and their activities have clear benefits for the individual as a consumer and a user of public services. If collected accurately and used properly databases of personal information can support both 'de-personalised', impartial decision-making processes and the delivery of 'personalised' services tailored to the needs of the individual. (Paragraph 123)

8. However, the risks associated with the collection and use of personal information in databases in particular and the monitoring of individuals' behaviour in general, should not be underestimated. Mistakes or misuse of data can result in serious practical harm to individuals. Those less demonstrable risks which relate to the erosion of one's sense of privacy or individual liberty also have a practical aspect and a broad application in that they affect the way in which citizens interact with the state. (Paragraph 124)

9. The risks associated with surveillance increase with the range and volume of information collected. The Government has a crucial role to play in maintaining the trust of the public: any evaluation of the use of surveillance must take into account the potential risk to this relationship with the public. (Paragraph 125)

10. Technological capabilities continue to expand, increasing our means both of generating information about ourselves and of using that information for different purposes. But the drive to make the most of these capabilities should be tempered by an evaluation of the risks involved in collecting more information. Particular consideration should be given to situations in which individuals might suffer as a result of their lack of awareness or ability to take advantage of opportunities to exercise choice over how information about them is used, or to check that it is accurate. (Paragraph 126)

Are existing safeguards strong enough?

11. We welcome efforts to develop technological means by which organisations and individuals can protect personal information and prevent unwarranted monitoring of individuals' online activities. We recommend that the Government track and make full use of new developments in encryption and other privacy-enhancing

technologies and in particular those which limit the disclosure and of collection of information which could identify individuals. We further recommend that the resources of the Information Commissioner's Office be expanded to accommodate sufficient technical expertise to be able to work with the Chief Information Officer to provide advice on the deployment of privacy-enhancing technologies in Government. (Paragraph 159)

12. We recognise, however, that awareness of and access to privacy-enhancing technologies is not universal amongst the public. Over-reliance on the capacity of technology to secure data systems leads to neglect of the need to ensure that processes for the management of information by organisations are robust. It also raises unrealistic and potentially discriminatory expectations of individuals who are not in a position to take steps to prevent the theft of their personal information. (Paragraph 160)

13. Where individuals have little or no choice about providing personal information, such as in their interactions with Government, it is especially important that the organisation which collects and holds the information takes responsibility for safeguarding it, rather than attempting to pass on the responsibility to the individual. The organisation's responsibility should begin before collection takes place: by obtaining consent for collecting and processing data where possible and by providing an explanation where this is not possible. (Paragraph 161)

14. 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. The Home Office should highlight the distinction between those areas in which individuals can exercise choice by giving or withholding their consent, and those areas in which seeking informed consent is not feasible and transparency is particularly important. (Paragraph 162)

15. 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 personal information. We recommend that the Government adopt a principle of data minimisation in its policy and in the design of its systems. We further recommend that the Government acknowledge the distinction between identification and authentication as one which is valuable in its efforts to adhere to this principle. (Paragraph 163)

16. It is not just the volume of data collected that creates a problem: the longer information is retained, the more likely it is that the information will be out of date and inaccurate. Information should be held only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes rather than service delivery it should normally be anonymised and retained only for a previously specified period. (Paragraph 164)

17. We welcome the reviews commissioned by the Government to improve data security, particularly in relation to information-sharing. We expect the Government to make full use of the opportunity these reviews provide to reassess the adequacy of the definitions and principles set out in the Data Protection Act. Such a reassessment

should be carried out not only in light of recent data loss incidents but also against the challenges presented by increases in the collection, storage and sharing capability of information systems and intensification in criminal activity associated with the misuse of personal information. The Home Office must act as a matter of urgency to tackle these challenges. (Paragraph 189)

18. Any increase in the collection and storage of information increases the risk that security will be breached and that information will be used for purposes other than those for which it was collected. In keeping with a principle of data minimisation, more rigorous risk analysis of systems already in place must be carried out before new techniques for collecting information are deployed or new databases planned. The decision to create a major new database, share information on databases, or implement proposals for increased surveillance should be based on a proven need. (Paragraph 190)

19. We commend the Information Commissioner for his work on Privacy Impact Assessments and support his drive to ensure that Government and others undertake thorough evaluation work in relation to the benefits and risks of surveillance. We also acknowledge that if published, in providing individuals and interest groups with details about surveillance activities which would not otherwise be made available, PIAs could help to raise awareness of the issues the Information Commissioner has sought to highlight. (Paragraph 191)

20. We are concerned, however, that PIAs might be regarded simply as bureaucratic exercises, and that they would be undertaken not before and during the design phase of any system but afterwards; by which time their value as a practical risk assessment tool would have been lost. For PIAs to be effective they should be used to carry out preliminary risk analysis for a new project before the design phase begins. For Government departments and agencies this preliminary risk analysis should culminate in a summary statement, to be signed off by the Information Commissioner or otherwise subject to independent audit. The statement should set out the benefits of a new system against the risks posed by collecting, storing and using the information required by the system. (Paragraph 192)

21. Every system for collecting and storing personal information should be designed with a focus on security and privacy. The design process should involve planning not only in relation to the technical aspects of access to systems but also to the staff management protocols for access and information-handling. (Paragraph 193)

22. Every system for collecting and storing data is susceptible to unauthorised access, misuse and theft. For existing and proposed systems the Government should specify what it considers to be an acceptable level of failure and develop contingency plans to mitigate the damage caused by leaks or theft of data. (Paragraph 194)

23. The weakest aspect of a system may be the establishment and enforcement of protocols for access and use rather than any technological safeguard. Organisations which manage such systems must take full responsibility for limiting access to databases and the information they contain and for enforcing procedures for sharing and transferring data. We support the Information Commissioner's call for an

extension of his inspection and audit powers to facilitate the strengthening of these procedures across Government and the private sector. Tougher penalties for negligent information-handling should be introduced in order to make clear where the burden of responsibility lies. (Paragraph 195)

24. A privacy officer or director of data security should be assigned by departments to take responsibility for risk analysis and to report to the Permanent Secretary on the privacy implications and safeguards of each project which involves the collection or sharing of personal information. (Paragraph 196)

25. The Home Office should publish a report on an audit of the data collections managed by the Department and its agencies, outlining as far as possible without compromising security the technological and procedural safeguards currently in place. (Paragraph 197)

What role does surveillance play in the work of the Home Office and the fight against crime?

Camera surveillance

26. Under camera surveillance in public spaces, individuals have very little control over whether or not their images and movements are captured and over how they are stored and used. This lack of choice intensifies the obligation on camera operators and regulators to behave responsibly and to deploy surveillance technology only where it is of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty. (Paragraph 221)

27. We acknowledge the popularity of CCTV schemes and do not underestimate the potential effect on crime levels of successful attempts to encourage people to use public spaces. However, as the Minister told us, it has been difficult to quantify the benefits of CCTV in terms of its intended effect of preventing crime. We recommend 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. (Paragraph 222)

28. We welcome the drive to create standards for the use of camera surveillance in order to enhance the value of the images captured in the fight against crime. We recommend that the Home Office work with the police to increase public awareness and manage public expectations of camera surveillance. (Paragraph 223)

29. Whilst we share the reservations of the police about unfettered public access to surveillance cameras, we endorse the Information Commissioner's calls for greater transparency in relation to camera surveillance and recommend that the Home Office take steps to facilitate access to footage in certain circumstances, for example where an individual is seeking to eliminate him or herself from police enquiries. (Paragraph 224)

30. The continued value and popularity of CCTV depends on continued public confidence that camera operators are acting responsibly and that the Government, in regulating CCTV schemes, is mindful of concerns about privacy. We note that the Minister saw the fact that much CCTV footage is held for a limited period of time as a barrier to the development of a surveillance state. In designing camera schemes operators should consider how long images need to be stored and the Home Office should support a principle of data minimisation in this respect. (Paragraph 225)

31. We acknowledge that technological developments have significantly increased the potential of camera surveillance in terms of crime detection. However, the Government should evaluate the impact of each major development for its effect on individual liberty. In particular, the Home Office should give its assurance that it will not countenance schemes such as those which involve the use of microphones attached to cameras, and in effect apply the techniques of directed and intrusive surveillance to the general public. Such measures impinge on the degree of privacy individuals expect to be able to enjoy in public spaces and the Home Office must take responsibility for guarding against this kind of constraint on individual liberty. (Paragraph 226)

National Identity Scheme

32. We have not sought in our inquiry to revisit the debate on the merits of identity cards. We are concerned, however, about the potential for 'function creep' in terms of the surveillance potential of the National Identity Scheme. Any ambiguity about the objectives of the Scheme puts in jeopardy the public's trust in the Scheme itself and in the Government's ability to run it. Whilst we accept the Government's assurance that the Scheme will not be used as a surveillance tool, we seek the further assurance that any initiative to broaden the scope of the Scheme will only be proposed after consulting the Information Commissioner and on the basis that proposals will be subject to parliamentary scrutiny in draft form. (Paragraph 236)

33. We recommend that the Home Office produce a report on the intended functions of the National Identity Scheme in relation to the fight against crime, containing an explicit statement that the administrative information collected and stored in connection with the National Identity Register will not be used as a matter of routine to monitor the activities of individuals. (Paragraph 237)

34. We note the distinction drawn by the Minister between the National Identity Scheme and "the most lamentable of government IT projects" and agree that staged implementation provides a degree of protection against security breaches. Nevertheless, the Home Office must plan for security breaches and in particular it should examine the consequences of theft of the biometric information which forms part of the NIR. (Paragraph 245)

35. Taking into account the effect of recent data loss incidents on public confidence in the Government as a guardian of personal information, we recommend that the Home Office submit more detailed plans for securing the NIR databases and a broad outline of contingency plans to be implemented in the event of a loss or theft of

biometric information from databases managed by the Identity and Passport Service, for comment by the Information Commissioner. (Paragraph 246)

36. Recent data loss incidents have involved failures not of technology but of policy in that those who had access to the information in question did not observe proper procedures for the handling and sharing of data. The Minister's assurances that the Government has learned lessons, though welcome, are not sufficient to reassure us or, we suspect, the public. Access to NIR databases should be strictly limited and governed by clear protocols, which should be developed in consultation with the Information Commissioner. We recommend that the Home Office publish a detailed account of its plans for NIR access procedures. (Paragraph 247)

37. The Home Office should address the Information Commissioner's concerns about the administrative information to be collected as part of the NIR. We accept that the Government's intention is to create an 'audit trail' to regulate access to NIR databases, but we are concerned about large stores of information about individuals' transactions and activities, particularly if registration is to become compulsory. (Paragraph 248)

38. We recommend that the Home Office publish its plans for collecting and retaining administrative information as part of the NIR and that it commit to a principle of data minimisation for the National Identity Scheme. We seek assurance from the Home Office that it has taken full account of the potential of advanced privacy-enhancing technologies to reduce the amount of information it is necessary to collect in order to authenticate transactions and prevent fraud and unauthorised access. (Paragraph 249)

39. We note that the Home Office has no plans to publish any specific privacy impact assessment of the National Identity Scheme. In terms of the design of the Scheme it is much too late for such an assessment to serve the intended purpose of integrating privacy considerations with the Government's plans to collect and store information. We recommend that on proposing any change in policy on the collection, storage, sharing or use of National Identity Register data, the Home Office make a report to Parliament on the implications of the change for an individual's privacy. The report should address the following questions: how much extra information will be collected? For how long will it be stored? How many more people will have access to it? For what new purpose will it be used? (Paragraph 250)

National DNA Database

40. We recognise the National DNA Database as a valuable investigative tool, particularly in relation to police efforts to solve older cases. But the sensitive nature of the information which may be yielded by DNA heightens the degree of responsibility borne by the Government. The Home Office must work with the National Policing Improvement Agency and the police to set and observe a regulatory framework which protects individuals from unnecessary invasions of privacy and loss or unauthorised use of their genetic material and information gleaned from it. (Paragraph 281)

41. The Home Office should actively support the NPIA in its efforts to reduce the rate of replication on the NDNAD. Inaccuracies in the information on the database must be corrected to enable the police and the public to reap the full benefit of the NDNAD. (Paragraph 282)

42. We welcome the Government's assurance that the National DNA Database will not be used in any attempt to correlate particular genetic characteristics with propensity to commit crime. We recommend that the Home Office renew this assurance in conjunction with the Government's conclusions on the review of the Police and Criminal Evidence Act. We recommend that the Home Office make public at the earliest stage any plans to revisit this issue. (Paragraph 283)

43. The Government's consultations should help to clarify the purposes and processes of DNA collection and retention. We endorse the views of the NPIA and the Minister that these purposes and processes must be transparent in order to maintain confidence in the database as a proportionate response to crime. (Paragraph 284)

44. There have been calls for an expansion of the National DNA Database to include profiles connected with non-recordable offences and for a 'universal database' and for the Government to reconsider its policy on retaining the profiles of those who have been arrested but not charged. In order to facilitate a full debate and an appropriate level of Parliamentary scrutiny we recommend that alongside any conclusions of the PACE review the Government introduce primary legislation to replace the current regulatory framework for the National DNA Database. We recommend that this legislation provide for a more accessible mechanism by which individuals can challenge the decision to retain their records on the Database. (Paragraph 285)

45. The Government should reconsider the ways in which National DNA database information is collected, handled, stored and transferred. In particular we recommend that in order to minimise the data held, the Home Office and the police should review the identifiers used for samples and the policy of retaining samples. (Paragraph 286)

The potential of other public and private sector databases for use in the fight against crime

46. In its use of databases and other means of collecting, storing and using personal information the Home Office should explicitly address these questions: in the context of the fight against crime where should the balance between protecting the public and preserving individual liberty lie? How should this balance shift according to the seriousness of the crime? What impact will this have on the individual and on our society as a whole? (Paragraph 305)

47. Even as society confronts its most serious threats it must protect its liberties. The fight against crime in general does not provide sufficient justification for information-sharing which might have an impact on privacy. It is vital that before information is shared for purposes other than those for which it has been collected those purposes are subjected to the closest scrutiny. (Paragraph 306)

48. Information-sharing must only be carried out in the context of a robust statutory framework which incorporates tests of proportionality and mandates the securing of consent where possible. The effectiveness of information-sharing should be assessed at the stage at which a new project is proposed, in order to prevent unnecessary sharing and retention of data. We recommend that where the sharing or matching of information held by the Home Office or its agencies is proposed, the Information Commissioner should act as a consultee and mediator on the same footing as the Ministry of Justice. (Paragraph 307)

49. Exemptions from the Data Protection Act notwithstanding, in giving consent and choosing services individuals are better informed about how their information is used and shared in the private sector than they are about how it might be used and shared by the Government. We recommend that the Home Office work with the Information Commissioner to raise awareness of how information generated in the private sector—such as details of retail purchases, or information posted on blogs or social networking sites, for example—might be used in the investigation of crime. (Paragraph 308)

50. We welcome the Minister's reassurance that the Government is not interested in "fishing" for information about individuals. However, we do not underestimate the lure of new technological capabilities and new ways of sharing and matching information from a range of sources, which might appear to offer benefits in the fight against crime. The Home Office should exercise a 'self-denying ordinance' in relation to its use of technological capabilities and its power to collect personal information. (Paragraph 309)

51. We would be particularly concerned by any attempt to use patient data or information held on children for the purposes of predictive profiling for future criminal behaviour rather than child protection: the Home Office must not undertake or sponsor work of this sort. (Paragraph 310)

Regulation of Investigatory Powers Act

52. We recognise the distinction drawn by the Minister between the degrees of intrusion caused by the interception of communications and access to communications data. In our view, however, access to communications data by a relevant authority has a significant impact on an individual's privacy. We note the increase in requests for access to communications data in recent years and the large number of organisations empowered by RIPA to make such requests. Whilst communications traffic continues to increase and diversify, the provisions of RIPA in respect of communications data are not well understood. We recommend that the Home Office use the opportunity afforded by the latest review of RIPA codes of practice to take steps to raise public awareness of how and why communications data might be collected and used. (Paragraph 331)

53. For each new organisation authorised under RIPA to request access to communications data, the Home Office should produce a statement setting out the purposes for which the data will be used and evidence that access to communications data represents a proportionate response in terms of the problem to be addressed

and the impact on individual privacy. Any assessment carried out by the Home Office should apply a test of proportionality: a potential intrusion which might be justified by the need to investigate terrorism would not be justified by efforts to tackle minor crimes such as littering. (Paragraph 332)

54. We note in the context of debate on the application of RIPA authorisations, the range of views on whether or not actions such as adjusting CCTV cameras constitute surveillance as defined by the Act. We also have serious concerns about the deployment of surveillance in relation to less serious crimes, which have been raised by—amongst other things—the use of RIPA powers to establish the validity of an application for admission to a school. The Home Office should undertake a public consultation on the levels of authorisation which should be required for various surveillance activities and the purposes which would justify different levels of intrusion. (Paragraph 333)

55. We are concerned by the implications for Members of Parliament of the events investigated by Sir Christopher Rose. Constituents must be able to speak freely to their Members of Parliament without fear of intrusion by the state. We reserve the right to return to this issue in due course. (Paragraph 334)

Annex: technological developments

This annex sets out some key technological developments in terms of surveillance capability, drawing on the work of the Surveillance Studies Network and the Royal Academy of Engineering and to the comments of our witnesses. We looked not only at significant changes in recent years but also at how these and other changes might affect how information about people and their activities is collected, stored and used in the near future.

The Surveillance Studies Network has identified five key areas in which the rapid development of technology has "helped to change the nature of surveillance": telecommunications, video surveillance, databases, biometrics and locating, tagging and tracking technologies.[336]

Telecommunications

The Surveillance Studies Network argues that throughout the last two decades, technological development and change has led to a diversification in the kinds of technology used for telecommunications. As examples of these new kinds of technology, the Surveillance Studies Network provides the following:

> Radio frequency devices now enable large-scale cellular or mobile telephony; optical fibre cabling enables high-speed digital fixed internet connection, and a combination of both enable wireless computing. Mobile telephony delivers not only voice calls, but text, image and video messaging, as well as location-based services. Internet technologies enable both asynchronous communications such as email, bulletin boards and newsgroups, as well as synchronous communications such as chatrooms, instant messaging and webcam/video messaging.[337]

Technological developments have also allowed these different means of communicating to converge and become interoperable so that internet connection can be made via mobile phones and calls can be made via desktop computers. The Surveillance Studies Network points out that the exchange of signals or data between devices which is required for these technologies to work "generates the mechanisms for the capture, monitoring and storage of information about that exchange".[338]

Video surveillance

Alongside the growth in the extent and scale of video surveillance, the Royal Academy of Engineering says that concerns arise from "the shift to digital technology, which has enabled two significant developments":

336 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 17

337 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 18

338 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 18

> First, digital recording capacities mean that images can be stored indefinitely, searched digitally, analysed, reproduced and manipulated with increasing ease. Second, images from any camera can be made available instantly to anyone with the capacity to receive data in this form.[339]

Technological developments allow cameras to be linked as a network, and their footage to be streamed to the internet or television. They also allow footage to be stored digitally and searched automatically.

Biometrics

A biometric is a measurement of a biological characteristic such as fingerprint, iris pattern, retina image, face or hand geometry; or a behavioural characteristic such as voice, gait or signature. Biometric technology uses these characteristics automatically to identify individuals whose biometrics have been stored on a database.[340] Now used on passport and identity card systems, biometric identifiers are used in border controls and as an access gateway to information and services. The Surveillance Studies Network pinpoints the attraction of biometric systems:

> The idea is that accuracy will be increased and fraud reduced. PINs and passwords may be forgotten or lost, but the body provides a constant, direct, link between record and person.[341]

The Surveillance Studies Network notes in particular the development of face recognition software.[342] Facial recognition maps various features on the face, for example, the distances between eyes, nose, mouth and ears.[343] The measurements are digitally coded and this can then be used for comparison and verification purposes. The Surveillance Studies Network says that whilst facial recognition and other biometric video-linked surveillance systems "still face major technical obstacles in operating outdoors on city streets", "considerable research and development investment is rapidly addressing these".[344]

Locating, Tracking and Tagging technologies

The development of devices which can track the movements of good and people has been identified by the Surveillance Studies Network as another significant technological change. The Royal Academy of Engineering points out that "As long as it is switched on, a person's mobile phone can reveal where they are, within a range of 150–400 metres in urban

339 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 33

340 *Biometrics and security*, POSTnote 165, Parliamentary Office of Science and Technology, November 2001

341 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 24

342 Surveillance Studies Network, A Report on the Surveillance Society: Full Report: revised with a new Postscript (March, 2007), p 24

343 Identity and Passport Service, *Biometric passports*. Available at: http://www.ips.gov.uk/passport/about-biometric-why.asp

344 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 24

areas."[345] Geographical Information Systems can be used to combine data from database and satellite or other technologies and to visualise the movements of people, vehicles and goods.[346]

Radio Frequency Identification (RFID) tags are small wireless devices that provide unique identifiers which can be read by remote sensors. Identity Cards and other documentation (such as the 'Oyster' travel cards issued by Transport for London) may now contain RFID tags. Tags on 'e-Passports' (issued in the UK since spring 2006) contain the information and picture from the identification page of the passports. The information can be retrieved by passing the passport over a reader.[347] Newer, 'active' RFID tags emit signals over a greater range and can be sensed remotely.[348]

A further change which the Surveillance Studies Network says "has occurred subtly and largely unnoticed" is the implantation of living beings with chips. Animals such as racehorses and household pets, and humans (a group of around 70 people with degenerative brain conditions were implanted to enable carers to locate them easily), have been implanted.[349]

Future developments

According to the Royal Academy of Engineering, all of the technologies that will have an impact on the mass market in the next five to ten years already exist, whether they are already widely available or are used only by a small number of people. In its report on *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, the Royal Academy of Engineering outlines a "technology roadmap" to set out "how technologies for collecting, storing and processing data are likely to evolve over the next five to ten years".[350] In order to highlight key trends, the Royal Academy of Engineering organises the technologies in three "layers":

- Connection technologies: technologies that affect how organisations move data around as well as how they deliver information and services to customers. Improvements in connection technology have the potential to widen the distribution of products and services and lower transaction costs. Examples of connection technologies include RFID, webcam and wifi.

345 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 34

346 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 24

347 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 17

348 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 17

349 Surveillance Studies Network, *A Report on the Surveillance Society: Full Report: revised with a new Postscript* (March, 2007), p 25

350 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 14

- Disconnection technologies: technologies that provide access control to services and resources, to maintain the security of data. Examples include fingerprint, face and iris recognition, mobile phone SIMs and other tamper-resistant tokens or cards.

- Processing technologies: technologies that affect how data are handled within organisations. A search engine is an example of a processing technology, as is multi-media memory card (MMC) technology.[351]

The Royal Academy of Engineering draws attention to the differences between these layers and in particular to the implications of those differences for the effect of technology on surveillance. If connection technologies are analogous to doors, it argues, disconnection technologies are analogous to locks:

> Most importantly, while connection is easy disconnection is difficult. That is to say, it is relatively simple to create a network between a set of computers, but it is difficult to partition the data on a computer within a network so that the data can only be accessed by certain computers or users. Disconnection will obviously be crucial to privacy and security of data.[352]

Professor Ross Anderson suggested that recent trends—the use of RFID technology, the incorporation of communications technology in an increasingly diverse range of devices, and the interoperability of these devices—would intensify:

> what we are going to see is probably a move to a world in which more and more objects are a little bit like computers. In 10 years' time, most things that you buy for more than about a tenner and which you do not eat and drink will have got some kind of CPU and communications in them and even things that you buy to eat or drink may have RFID tags on them … Fifty or sixty years ago, there were a handful of computers and now we have several computers on our person, mobile phones, laptops, iPods et cetera, and that will go up from a few to dozens. Your car might now have 30 computers in it and it might have 100 in it within 10 years' time and many of these computers will talk to each other.[353]

Pete Bramhall, Manager of Privacy and Identity Research at Hewlett-Packard Laboratories told us that new developments would take place in a context in which "the privacy issues remain the same and the principles for how one should address those privacy issues will also remain the same". The challenge for system designers, he said, would be:

> remembering to take account of those principles and not just getting captivated and dazzled by the potential of what the technology could do.[354]

351 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), pp 14–16

352 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p 14

353 Q 187 (Professor Anderson)

354 Q 189 (Pete Bramhall)

Formal Minutes

Tuesday 20 May 2008

Members present:

Rt Hon Keith Vaz, in the Chair

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

Draft Report (A Surveillance Society?), proposed by the Chairman, brought up and read.

Ordered, That the Chairman's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 334 read and agreed to.

Annex (Ground rules for Government) agreed to.

Annex (Technological developments) agreed to.

Summary agreed to.

Resolved, That the Report be the Fifth Report of the Committee to the House.

Ordered, That the Chairman make the Report to the House.

Written evidence was ordered to be reported to the House for printing with the Report.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Written evidence was ordered to be reported to the House for placing in the Library and Parliamentary Archives.

[Adjourned till Tuesday 3 June at 10.15 am

Witnesses

Tuesday 18 March 2008

List of written evidence

List of unprinted evidence

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

Michael Nettleton
Christine Bloomfield
David Moss
Autism Rights
David Muxworthy
Nuffield Council on Bioethics
Angela Pinter
Jade Smith
Dr Mark Viney

List of Reports from the Committee during the current Parliament

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

Session 2007–08

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

Session 2006–07

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

Session 2005–06

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