House of Commons

Justice Committee

Protection of Private Data

First Report of Session 2007–08

Report, together with formal minutes, oral and written evidence

Ordered by The House of Commons
to be printed 17 December 2007

HC 154
Published on 3 January 2008
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The Justice Committee

The Justice Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Ministry of Justice and its associated public bodies (including the work of staff provided for the administrative work of courts and tribunals, but excluding consideration of individual cases and appointments, and excluding the work of the Scotland and Wales Offices and of the Advocate General for Scotland); and administration and expenditure of the Attorney General's Office, the Treasury Solicitor's Department, the Crown Prosecution Service and the Serious Fraud Office (but excluding individual cases and appointments and advice given within government by Law Officers).

Current membership

Rt Hon Alan Beith MP (Liberal Democrat, Berwick-upon-Tweed) (Chairman)
Rosie Cooper MP (Labour, West Lancashire)
David Howarth MP (Liberal Democrats, Cambridge)
Siân James MP (Labour, Swansea East)
Daniel Kawczynski MP (Conservative, Shrewsbury and Atcham)
Jessica Morden MP (Labour, Newport East)
Julie Morgan MP (Labour, Cardiff North)
Humfrey Malins MP (Conservative, Woking)
Rt Hon Alun Michael MP (Labour Co-op, Cardiff South and Penarth)
Robert Neill MP (Conservative, Bromley and Chislehurst)
Dr Nick Palmer MP (Labour, Broxtowe)
Virendra Sharma MP (Labour, Ealing Southall)
Andrew Tyrie MP (Conservative, Chichester)
Dr Alan Whitehead MP (Labour, Southampton Test)

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

Publications

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/justicecom

Committee staff

The current staff of the Committee are Roger Phillips (Clerk), Dr Rebecca Davies (Second Clerk), Ruth Friskney (Adviser (Sentencing Guidelines)), Maik Martin (Committee Legal Specialist), Ian Thomson (Committee Assistant), Jane Trew (SPIRE Pilot Manager), Chryssa Poupard (Secretary), Henry Ayi-Hyde (Senior Office Clerk), Gemma Buckland (Home Affairs/Justice Public Policy Specialist) and Jessica Bridges-Palmer (Committee Media Officer).

Contacts

Correspondence should be addressed to the Clerk of the Justice Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 8196 and the email address is justicecom@parliament.uk

Media enquiries can be addressed to Jessica Bridges-Palmer, Committee Media Officer, House of Commons, 7 Millbank, London SW1P 3JA. Telephone number 020 7219 0724 and email address bridgespalmerj@parliament.uk

Contents

Report

1 Problems with data protection

Handling personal data

1. On 20 November 2007 the Chancellor of the Exchequer told Parliament that HM Revenue and Customs (HMRC) had lost two CDs containing personal and banking information belonging to all child benefit claimants. In total, the loss of these discs affected about 25 million people. It is too early to know exactly what the impact of this loss will be on the families affected, but there are clearly major risks in connection with identity theft. This error was compounded by the fact that HMRC sent out 7.25 million personalised letters of apology for the CD data loss which contained the relevant child benefit claimant's name, address, national insurance and child benefit numbers. There is a grave risk that these letters holding personal data could be used for identity theft if they fell into the wrong hands.

2. We immediately decided to take evidence from Richard Thomas, the Information Commissioner, and David Smith, his Deputy who takes the lead on Data Protection issues, about this case and about the issue of protection of personal data held by Government and other agencies. Speaking of this particular case, the Information Commissioner said:

> "There is no doubt that everybody concerned recognises the seriousness of [the] situation. It is unprecedented, in our experience. From what I know so far, [it is] a really shocking example of loss of security; the scale of it, I think, is well beyond anything we had considered before. All the previous examples I shared with you pale into insignificance…compared to the scale of this particular incident, with 25 million individuals concerned, and I think over 7 million families. Clearly, there are risks in connection with identity theft and the like if banking information were ever…to get into the wrong hands."[1]

3. We are gravely concerned that this incident is not an isolated example – except, perhaps, in terms of the scale of its impact, both because of the number of people involved and the sensitivity of the data.[2] The Information Commissioner had referred to the risks involved in the way in which personal data was handled in his Annual Report for 2006/07:

> "Recent security breaches—permitting the wrong people to access confidential information—provide a powerful illustration of the need to ensure that safeguards are achieved in practice. The roll call of banks, retailers, Government departments, public bodies and other organisations which have admitted serious security lapses is frankly horrifying."[3]

In oral evidence to us, he said:

> "… when we published the annual report, it was mid July, and as you have noted […] we highlighted a number of really quite worrying security breaches that had come to

1 Q.3

2 Q.40

3 ICO, *Annual Report 2006-07*, Foreword by Mr Richard Thomas, p. 7

> our attention during the course of the last year. So I thought it appropriate then to sound a very loud warning about the need to take security and other data protection safeguards ever more seriously…We had a number of cases, both private sector and public sector, where quite serious breaches had occurred. You may recall we came across 12 major clearing banks which had been dumping paper waste in rubbish bags which had been accessible to the public in High Streets and the like. We came across a retailer where credit card transactions had gone adrift. We were dealing with the NTS, an agency of the Department of Health, which had a website where doctors applying for positions were able to see the applications made by other doctors. And we were investigating a case involving the Foreign Office, where visa applicants from India, Russia and elsewhere in the world using an online system were able to see the applications for visas made by other applicants."[4]

In evidence to the Treasury Committee, the acting Chairman of HMRC admitted that there was a "systemic" failing in the handling of personal data.[5]

4. Similar concerns were raised two years ago by Dr Mark Walport, who is now heading the Government's main review of data protection and the use of personal information. He co-authored a report for the Council for Science and Technology (CST), an independent Government advisory body, which warned that departments needed to "streamline data protection protocols" and improve security in the context of data sharing. The report, *Better use of personal information: opportunities and risk,* published in November 2005, was commissioned by the Government for the then Prime Minister, Rt Hon Tony Blair MP. It predicted that the unauthorised use of personal data would "damage [the] Government's reputation—with political ramifications".[6]

5. In relation to intra-Government data sharing for statistical and research purposes, Dr Walport's report noted that:

> "The legislative regime is critical to this area, but it is complex and not well understood, in particular the Data Protection Act. Greater clarity is needed urgently: the large amount of guidance, often at a Departmental level, serves simply to confuse. In parallel, Government should look again at whether, and if so what, legislative changes will be necessary to promote sharing of, and access to, personal data for researchers and statisticians. Governance of data management systems is a central issue: the contractual relationship between those who share data needs to be clear and explicit."[7]

6. Clearly, the HMRC case has had a major impact on Government Departments. The Cabinet Secretary has been asked to carry out a review and a trawl is being conducted throughout Departments for information about the way in which data is being protected.[8] The Information Commissioner told us that quite a number of organisations, both public and private sector, had approached his office, almost "on a confessional basis", to bring to

4 Q.1

5 Evidence to the Treasury Committee, Session 2007-08, HC 57-ii, Qq. 173-174

6 Council for Science and Technology, *Better use of personal information: opportunities and risk*, November 2005

7 ibid., p 2

8 Q.5

his attention problems they had encountered with security inside their own organisations, although none of these cases appeared to be on anything like on the scale of the one involving HMRC and Child Benefit claimants.[9]

7. The Information Commissioner was rightly reluctant to be drawn into making any statement about the HMRC case, on the basis that the matter was still being investigated.[10] However, it was obvious to him and his Deputy that there were some questions which needed to be answered. In particular, any review would have to show how the system allowed a junior official to download so much data at once. At first glance, he thought that such an event suggested not just bad organisation but a lack of technical measures to protect the data. This raised important issues about the cultural approach to security and whether this was taken seriously all the way through the organisation from the most senior management downwards.[11]

8. **We are extremely concerned to hear from the Information Commissioner that there are more cases involving the loss of personal data which have not yet fully come to light. The warning which he issued in the summer about the dangers of mishandling personal data and the extensive security lapses in a wide range of organisations has been proved correct.**

Sharing information and adequate safeguards

9. In his *Speech on Liberty* on 25 October 2007, the Prime Minister, Rt Hon Gordon Brown MP, praised the benefits of cross-Government data flow and information sharing but also emphasised the need for adequate safeguards:

> "At the same time, a great prize of the information age is that by sharing information across the public sector—responsibly, transparently but also swiftly—we can now deliver personalised services for millions of people, something not dreamt of in 1945 and not possible even ten years ago. So for a pensioner, for example, this might mean dealing with issues about their pension, meals on wheels and a handrail at home together in one phone call or visit, even though the data about those services is held by different bits of the public and voluntary sectors. But if Governments do not insist on accountability where people's data is concerned—and are not held independently to account—then we risk losing people's trust which is fundamental to all these issues and more."[12]

10. As the Prime Minister has said, information sharing between Government Departments represents a great opportunity for improving the services given to the public. There are, however, substantial risks associated with large databases which contain personal data and which are open to large numbers of licensed users. Modern Government depends upon such databases, but the trend is for extending these considerably. We note, for example, that there is a new child protection database system called ContactPoint,

9 ibid.

10 Q.7

11 Q.8

12 Rt Hon Gordon Brown MP, Speech on Liberty, 25 October 2007, www.pm.gov.uk/output/page13630.asp

created in the wake of the Climbié inquiry, which has access rights granted to many thousands of people. The Government's plans for identity cards have attracted comment from the Information Commissioner, who has registered his disquiet both about the scale of data proposed to be kept and the length of time for which it will remain on file.[13]

11. The Government has acknowledged the need to think again about protection of data in connection with the identity card system. Michael Wills MP, Minister of State at the Ministry of Justice responsible for data protection, told the Joint Committee on Human Rights that:

> "We obviously are going to have to look at the National Identity Register again in the light of this. We will have to learn the lessons. I cannot tell you what they are now, but what I am absolutely certain about is that everything will have to be scrutinised. We will have to take evidence from the various reviews and then we will assess it again."[14]

12. Linked to issues of adequacy of data protection in the UK is the matter of data exchange and protection at EU level in the context of greater interoperability of Government databases, which the UK Government and those of other EU member states aspire to. The EU Framework Decisions incorporating the Prüm Treaty into EU law and establishing the 'principle of availability' of Government-held information between EU member state authorities will have a direct impact on the protection of data of UK citizens held by the UK Government. If data held by the Government is available for inspection outside the jurisdiction, then the importance of restricting the amount of data held, as well as proper policing of who had access to it, takes on even greater importance.

13. **The Government has acknowledged that there must be a proper approach to handling personal data. There must be a sensible balance between achieving the advantages which data sharing will provide and minimising the risks inherent in maintaining large databases to which a wide range of officials and others can gain access.**

13 ICO, *The Identity Cards Bill – The Information Commissioner's Concerns*, October 2005; and see Q. 42ff

14 Michael Wills MP, Joint Committee on Human Rights, uncorrected transcript, 27 November 2007, Q 32

2 Action to be taken

Reviews

14. It is too early to draw firm conclusions about the action to be taken on the basis of the HMRC case. We note that the Government has started a series of reviews, which are largely independent of each other – some of which pre-date the HMRC case.[15]

Review of the framework for using data

15. In his speech on Liberty referred to above, the Prime Minister announced a wide ranging review of data sharing and data protection:

> "Jack Straw and I have asked the Information Commissioner, Richard Thomas and Doctor Mark Walport, Director of the Wellcome Trust, to undertake a review of the framework for the use of information—in both the private and public sector—to assess whether it is right for today's landscape and strikes the right balance—giving people the protection they are entitled to, while allowing them to make the most of the opportunities which are being opened up by the new information age."[16]

This Review was established before the HMRC case had come to ministers' attention.

Review of data protection across Government

16. In addition to the Thomas/Walport Review, there has been a review of data protection practice across Government by Robert Hannigan, head of intelligence, security and resilience in the Cabinet Office, who will draw up new guidelines for the Prime Minister. Mr Hannigan's review coincided with a separate study by the senior partner and chair of PricewaterhouseCoopers, Mr Kieran Poynter, into what went wrong at HMRC.[17] He has asked each permanent secretary to "identify compliance with policies and standards" in their departments and agencies and recommend improvements. He will then look at how data protection can be improved.[18]

Possible changes to the Law

17. Some changes to the law relating to the protection of data have already been mooted by various commentators, including the Information Commissioner.

---

15 Qq.5-7

16 Gordon Brown, *Speech on Liberty*, 25 October 2007. The data sharing review was launched on Wednesday 12 December

17 The terms of reference of Mr Poynter's review are: "to establish the circumstances that led to the significant loss of confidential personal data on child benefit recipients, other recent losses of confidential data and the lessons to be learned in the light of those circumstances; to examine HMRC practices and procedures in the handling and transfer of confidential data on taxpayers on benefit and credit recipients; the processes for ensuring that such procedures are communicated to staff and the safeguards in place to ensure that they are adhered to; the reasons those failed to prevent the loss of confidential data; and whether those procedures and processes are sufficient to ensure the confidentiality of personal data." (Rt Hon Alistair Darling MP, HC Deb, 28 November 2007, col 308)

18 The Times, *Careless data loss 'should be an offence'*, 24 November 2007; and see Dr Gus Hosein of Privacy International, in The Times, *New data law 'urgently needed'*, 21 November 2007

New reporting requirements

18. The Data Protection Act does not require companies to notify either the Information Commissioner's Office or those affected by the loss of data. There have been calls for legislation which would require bodies which lose information to inform members of the public who are placed at risk.[19] This included one from the House of Lords Science and Technology Committee which recommended that legislation should incorporate the following key elements:

- Workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data;
- A mandatory and uniform central reporting system;
- Clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it.[20]

19. In his written evidence to Home Affairs Committee inquiry into *A Surveillance Society?*, the Information Commissioner echoed these recommendations:

> "Allied to the call for a penalty to be introduced for breaches of the data protection principles, the Commissioner believes that consideration should be given to security breach notification obligations in the UK. These are used in other jurisdictions and involve the organisation which is the subject of a breach being obliged to tell those individuals affected by it such as those whose personal information is involved, as well as, in some cases, the regulator. Such obligatory notifications could, if applied sensibly, not only provide protection for individuals but would also help the Information Commissioner to take appropriate action where necessary."[21]

Strengthening the criminal law

20. The Information Commissioner has called for changes in the law to make significant security breaches—where they are reckless or repeated—a criminal offence. At the moment he can only take limited enforcement action.[22] The Commissioner has submitted a draft proposal for changes to data protection powers and penalties to the Ministry of Justice.[23]

21. Currently, criminal offences under the Data Protection Act 1988, such as that of unlawful obtaining or disclosing personal data, be it intentionally or recklessly, only exist in relation to ICO staff and persons and organisations *who are not the data controller*. There is currently no criminal offence of a data controller (such as a private business or a Government department) intentionally or recklessly disclosing personal information.

---

19 The Times, *New data law 'urgently needed'*, 21 November 2007

20 Fifth Report from the House of Lords Science and Technology Committee, Session 2006-07, HL Paper 165, *Personal Internet Security*, paras 5.55-5.57

21 ICO, additional evidence submitted to the Home Affairs Committee, *Inquiry into 'A Surveillance Society?'*, para 28

22 The Independent, *Richard Thomas: Individuals value their privacy – institutions do not*, 27 November 2007

23 ICO, additional evidence submitted to the Home Affairs Committee, *Inquiry into 'A Surveillance Society?'*, paras 23-26

Furthermore, the current criminal offences only cover individuals and non-Governmental bodies or organisations; Government departments or agencies cannot be held criminally responsible for data protection breaches.

22. The Criminal Justice and Immigration Bill, recently considered in a Public Bill Committee, will increase the penalties available for data protection offences (including custodial sentences), but will not introduce new categories of offences.

Office of the Information Commissioner

Enforcement powers

23. The Information Commissioner has regretted the lack of powers to carry out unannounced spot checks and inspections without the consent of the place or organisation to be inspected:

> "For some time I have been pressing the Government to give my office stronger powers under the Act to audit and inspect organisations that process people's personal information without first having to get their consent. Ultimately this will ensure better compliance with the law and protect people's data. The Prime Minister announced yesterday that my staff will be able to spot-check Government departments. We will work with the Ministry of Justice to confirm the detail on this—what we need are full audit and inspection powers, and not just for Government departments, but for every organisation, public and private, that processes people's personal information. It is essential that we are properly resourced to carry out this new function."[24]

24. We note that the House of Lords Science and Technology Committee's Report on Personal Internet Security recommended that "… the Government examine as a matter of urgency the effectiveness of the Information Commissioner's Office in enforcing good standards of data protection across the business community".[25] The Government rejected this recommendation, on the basis that "the current enforcement regime for data protection is fit for purpose" and that the current arrangements for consulting the Information Commissioner and powers.[26] However, following the HMRC case, the Prime Minister announced at Prime Minister's Questions on 21 November 2007 that:

> "We will give the Information Commissioner the power to spot-check Departments, to do everything in his power and our power to secure the protection of data. In other words, we will do everything in our power to make sure that data are safe."[27]

We hope that this change of heart will lead to powers quickly being provided through legislation.

---

24 The Independent, *Richard Thomas: Individuals value their privacy – institutions do not*, 27 November 2007

25 Fifth Report from the House of Lords Science and Technology Committee, Session 2006-07, HL Paper 165

26 Government Reply to Fifth Report From the House of Lords Science and Technology Committee, Session 2006-07, HL Paper 165, Cm 7234

27 HC Deb, 21 November 2007, col 1179

Funding

25. We have previously noted potential difficulties in relation to funding of the Information Commissioners Office and the need to provide him with proper resources.[28] In relation to his Freedom of Information work, the Information Commissioner, in his Annual Report 2006-07 noted "the current level of funding means that some cases are taking longer than we want".[29] When giving evidence to us of the possibility of being given a new power of inspection without consent, the Information Commissioner said:

> "I would say, I remain dissatisfied, because we cannot do these inspections without adequate resources. We cannot even do spot checks of Government departments on a de facto basis without the resources to do it. We have to provide the entire data protection activities of my office on a budget of £10 million a year."[30]

26. **We note the anomaly that the same basic registration fee of £35 is paid by individuals, small businesses, large companies and large government departments or agencies, and we consider that a graduated rate would be more appropriate, more likely to reflect actual costs, and more suited to providing an adequate income for the policing of data protection.**

28 see e.g. First Report from the Constitutional Affairs Committee, Session 2004-05, Freedom of Information Act 2000 - Progress towards Implementation, HC 79-I and –II, paragraph 116

29 ICO, *Annual Report 2006-07*, Foreword by Mr Richard Thomas

30 Q.25

3 Conclusion

27. The extensive use of personal data is increasingly a feature of modern Government. Personal data must only be held where there are proper safeguards for its protection. This will become more and more a problem as it becomes ever easier to share data both within the country and across borders.

28. It is clearly important for the information Commissioner to be given adequate support in order to carry out any wider role in connection with data protection which results from a change in the law. We note that he already considers that his resources are at a minimum.

29. **We shall return to the issue of data protection in due course. We draw to the attention of the House that:**

- **There is evidence of a widespread problem within Government relating to establishing systems for data protection and operating them adequately;**
- **It is widely accepted that it is necessary to have a substantial increase in the powers given to the Information Commissioner to enable him to review systems for data protection and their application - recent events have underlined the urgency of this; and**
- **There is a difficult balance to be struck between the undoubted advantages of wider exchange of information between Government Departments and the protection of personal data. The very real risks associated with greater sharing of personal data between Government Departments must be acknowledged in order for adequate safeguards to be put in place.**

Formal Minutes

Monday 17 December 2007

Members present:

Mr Alan Beith, in the Chair

Siân James	Dr Nick Palmer
Daniel Kawczynski	Virendra Sharma
Julie Morgan	Mr Andrew Tyrie
Alun Michael	Dr Alan Whitehead
Robert Neill	

Draft Report (Protection of Private Data), 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 29 read and agreed to.

Resolved, That the Report be the First Report of the Committee to the House.

Ordered, That the Chairman make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 15 January at 4.00 pm

Witnesses

Tuesday 4 December 2007

Page

List of written evidence

Reports from the Constitutional Affairs (now Justice) Committee during the current Parliament

Session 2007-08

First Special Report	The Creation of the Ministry of Justice: Government Response to the Committee's Sixth Report of Session 2006-07	HC 140

Session 2006–07

First Report	Party Funding	HC 163
	Government response	*Cm 7123*
First Special Report	Party Funding – Oral evidence from the Lord Chancellor on the role of the Attorney General	HC 222
Second Report	Work of the Committee 2005-06	HC 259
Third Report	Implementation of the Carter Review of Legal Aid	HC 223
	Government response	*Cm 7158*
Fourth Report	Freedom of Information: Government's proposals for reform	HC 415
	Government response	*Cm 7187*
Fifth Report	Constitutional role of the Attorney General	HC 306
Sixth Report	The creation of the Ministry of Justice	HC 466
	Government response	*HC 140*

Session 2005-06

First Report	The courts: small claims	HC 519
	Government response	*Cm 6754*
Second Report	The Office of the Judge Advocate General	HC 731
Third Report	Compensation culture	HC 754
	Government response	*Cm 6784*
Fourth Report	Legal Services Commission: removal of Specialist Support Services	HC 919
Fifth Report	Compensation culture: *NHS Redress Scheme*	HC 1009
	Government response	*Cm 6784*
First Special Report	Legal Services Commission's response to the Fourth Report on removal of Specialist Support Services	HC 1029
Sixth Report	Family Justice: the operation of the family courts revisited	HC 1086
Seventh Report	Freedom of Information—one year on	HC 991
	Government response	*Cm 6937*
Eighth Report	Reform of the coroners' system and death certification	HC 902
	Government response	*Cm 6943*

Oral evidence

Taken before the Justice Committee

on Tuesday 4 December 2007

Members present

Mr Alan Beith, in the Chair

Julie Morgan
Alun Michael
Dr Nick Palmer
Mr Virendra Sharma
Dr Alan Whitehead

Witnesses: **Richard Thomas**, Information Commissioner, and **David Smith**, Deputy Information Commissioner, gave evidence.

Q1 Chairman: Mr Thomas, and Mr Smith, welcome, for your very timely visit to us. We are always pleased to see you, but this is a particularly timely visit. In your annual report in 2006/7, you talked about a sea change in relation to information rights, and yet you yourself have listed numerous data protection violations at Government level, and said, "The roll-call of banks, retailers, Government departments, public bodies and other organisations which have admitted serious security lapses is frankly horrifying." You have said that Ministers, Permanent Secretaries, chairs and chief executives have to ensure that their organisations guarantee safeguards and the necessary self-restraint. It has not really been happening in certain quarters, has it?
Richard Thomas: Chairman, when we published the annual report, it was mid July, and as you have noted from the introduction of the annual report, we highlighted a number of really quite worrying security breaches that had come to our attention during the course of the last year. So I thought it appropriate then to sound a very loud warning about the need to take security and other data protection safeguards ever more seriously. You have quoted the words I was going to use in my introduction to you, the words we used in the annual report for the need for these topics to be taken very seriously at the top of every organisation. We had a number of cases, both private sector and public sector, where quite serious breaches had occurred. You may recall we came across 12 major clearing banks which had been dumping paper waste in rubbish bags which had been accessible to the public in High Streets and the like. We came across a retailer where credit card transactions had gone adrift. We were dealing with the MTAS, an agency of the Department of Health, which had a website where doctors applying for positions were able to see the applications made by other doctors. And we were investigating a case involving the Foreign Office, where visa applicants from India, Russia and elsewhere in the world using an online system were able to see the applications for visas made by other applicants. We were investigating some of these at the time, some had been resolved, some have been resolved since the time of our annual report, but yes, we were sounding a very loud warning. We are saying that already, there had been a sea change in attitudes; we had seen, if you like, data protection and, of course, Freedom of Information alongside that, being taken a great deal more seriously than the previous year. The comments that I made in that report did receive a great deal of publicity at that time. I have some of the newspaper articles which followed the publication of that report, and some of the headlines from the press at the time: "Top firms breaching privacy rules", "Wake up call from watchdog on lapses in privacy".

Q2 Chairman: We read your press cuttings too, Mr Thomas.
Richard Thomas: Just the headlines, to give you a flavour of some of the concerns we were voicing at that time.

Q3 Chairman: Do we have rather a problem, in that when something like this happens, the tendency is to say, "Oh, a junior official made a mistake and sent off something which affects 20 million people", when in fact there should be procedures, and in many cases are procedures, and sometimes officials are told, "Oh, we cannot go through all that, it is going to be too expensive to separate out the necessary data that has to be sent".
Richard Thomas: I think clearly, Chairman, you are now referring to the HMRC incident. I first became aware of this just two weeks ago, I was actually giving evidence to the House of Lords Select Committee on a surveillance society. As I came out of that Select Committee hearing, I was asked by an official to go and meet the Financial Secretary to the Treasury, Jane Kennedy, immediately. I met her within five minutes of finishing that Select Committee appearance, and she outlined to me the situation that they had come across at HMRC. I met the Chancellor of the Exchequer the following morning, which was Thursday, 15 November, and he and I exchanged words about what had gone on. He confirmed the seriousness of the matter, and I gave him advice as to what I thought should be done in that situation. He then made his statement to the House of Commons, I think the following Tuesday, and of course there has been very much in the public domain since that time. There is no doubt that

everybody concerned recognises the seriousness of that situation. It is unprecedented, in our experience. From what I know so far, really a shocking example of loss of security; the scale of it, I think, is well beyond anything we had considered before. All the previous examples I shared with you pale into insignificance, I think, compared to the scale of this particular incident, with 25 million individuals concerned, and I think over 7 million families. Clearly, there are risks in connection with identity theft and the like if banking information were to ever, God forbid, get into the wrong hands. I think it is too soon for any of us to know exactly what has happened in this particular situation. I read what I read in the newspapers, but I very much welcome the fact that the Chancellor has invited Mr Kieran Poynter, who is the chairman of PricewaterhouseCoopers, to carry out a full investigation into this incident, and draw attention to some of the wider lessons that might be learned from it. I have been in touch with Mr Poynter, indeed I spoke to his deputy this morning, and I understand that the investigation is now underway. They are intending to produce an interim report on 14 December, and then the full report in the spring. One point which I raised with the Chancellor before this was announced publicly was that I said that we really had to see a full copy of the report coming from PricewaterhouseCoopers; that was agreed, and that was included in the Chancellor's statement to the House of Commons and in the terms of reference. So when we get the report which PricewaterhouseCoopers will be preparing, we can then find out exactly what went wrong, we will have all the facts before us, and we can then decide what sort of action would be appropriate. I have indicated, and the Chancellor himself has accepted, that it is almost certain that there was a breach of the Data Protection Act. I think that is certainly going to be the case, but when we get the facts, we can decide what action to take. I have already indicated that an enforcement notice is the main sanction available to us in this situation.

Q4 Chairman: Now you find yourself in the situation of being required to deal with the stable door, not just after the horse has bolted, but also the entire racing stable has bolted, with really potentially very, very serious consequences. I come back to the point I was making, which is not an attempt to carry out the inquiry into this case, but do you think there is a more general problem that relatively junior officials carry out these tasks of sending data around, but this kind of thing is going to happen unless there are very clear rules and protocols, and a senior official cannot turn to a junior official and say, "Oh, that is going to be too expensive, it is too complicated to do that", the protocols have to be clear, as you have done in the Freedom of Information Act with some success, but they do not seem to have been successful here.
Richard Thomas: Well, in the statement which I issued on the day that this became public news, I said, "Searching questions need to be answered about systems, procedures and human error", so I think we need to find out, in this case, what happened, whether it was just down to human error, or whether the systems and procedures themselves are open to question. I do not want to prejudge the investigation into this particular incident, but I think the general point you are making, which is that one has to make sure that there are adequate safeguards in place right across the entire system, must be the right point to make. This is a requirement of data protection law, that appropriate security arrangements are in place. In a moment, I will ask David Smith, my deputy, to share with you the wording of the Data Protection Act, what we call the seventh principle, which sets out the requirements in data protection terms, but it is also a matter of self-interest. In my annual report, which you just quoted from, I recognise it is as much a matter of self-interest, the reputation of the organisation, political commercial reputations at stake; it is a matter of self-interest to get this right. At this moment, I would have to say if a junior official could allow this to happen, one needs to ask very searching questions indeed about the entire system. Prima facie, I would question whether anybody should be allowed to download an entire database of this scale without going through the most rigorous pre-authorisation checks. One would want to question why software was not in place to prevent the entire database being downloaded, and in those circumstances where it can be downloaded, what sort of processes and procedures were in place to prevent anything untoward happening.

Q5 Chairman: Since this case, have you had any more junior officials or medium level officials actually coming to you and to your staff asking for advice in situations like this?
Richard Thomas: Well, there has been a lot happening in the last two weeks, Chairman. As well as the PricewaterhouseCoopers investigation, the Cabinet Secretary has been asked to carry out a review, and I think one of his officials, Mr Robert Hannigan, is already trawling for information around Whitehall departments, and we have been in touch with Mr Hannigan about this. At the same time, quite a number of organisations, both public and private sector, have come to us saying that they think they have found a problem, to the extent we have almost said they are coming on a confessional basis to bring to our attention problems they have encountered with security inside their own organisations. I hasten to add that none appear to be on anything like the same scale as that involving HMRC, but I think there is certainly more to come out in the wash as we move forward.

Q6 Chairman: I was also interested in whether officials, aware of what went wrong in this case, are starting to question the instructions they get from above, to say, "Just a minute, am I going to be another junior official who is pilloried for having passed on data? Can I get independent advice as to whether I have adequate safeguards in place?"
Richard Thomas: I think and I hope that this incident has been a massive wake-up call to the very top of organisations, so my impression is that

Permanent Secretaries, and, in the private sector, Chief Executives and Chairmen, are really now at long last asking the questions to make sure that the proper arrangements are in place. And if they are not being given the reassurances that they require, then where problems come to light, they are starting to share those with us, and they are taking remedial action. Already, there are some signs that some projects are being put on hold, or that a freeze has been put on the transfer of data, at least in the short-term, while people look more closely at the implications.

Chairman: Dr Whitehead?

Q7 Dr Whitehead: You have mentioned that there are now effectively several reviews underway in this area. Do you think they should be brought together?

Richard Thomas: I do not think that is really one for me, Dr Whitehead. We are there with various statutory functions, promoting good practice, ensuring compliance with the law, investigating particular incidents when we can. In this particular case, given that we have extremely limited resources, it seemed to make sense for me to wait until PricewaterhouseCoopers had done their inquiry to make sure we got a full copy, not just the one made public, because I anticipate some of their report may have some confidential material in it about security arrangements, but we need to see the full report, and it has been agreed that we will see that. So I welcome that as the inquiry into the particular events at HMRC and the lessons to be learned from that, and we will take appropriate action once that is received. But I also welcome the fact that there is now a more searching scrutiny right across Whitehall departments, and it remains to be seen quite what that produces, but at least it does show that from the very top, these matters are being taken seriously, something which we have been saying for many, many years, and it has needed, very sadly, an incident, a catastrophe on the scale of the one that has happened at HMRC, to make people take this matter seriously. But I do not know that I would be able to comment on the merits or demerits of somehow amalgamating the various inquiries. What I did say to Mr Poynter, who I mentioned earlier, the Chairman of PricewaterhouseCoopers, was that not only did I suggest that our organisations should work closely together, but there is a third organisation, the Independent Police Complaints Commission, the IPCC, which has statutory functions in this area. I was in touch the same day with the Chairman of that, Nick Hardwick, and we have agreed to move forward on a tripartite arrangement. That is where matters are at the moment. So I think there is a good deal of what I would call sensible co-ordination going on.

Q8 Dr Whitehead: Would you suggest then that the sensible co-ordination might lead, as it were, to a sort of meta-inquiry outcome, that the different reviews that are being undertaken might feed into something which is of a piece in the end; or alternatively, would you see that there is a potential danger of particularly inquiries and reviews, as it were, saying particular things and then being perhaps at least in part contradicted by other inquiries, so that the net outcome is rather obscure, as opposed to clear.

Richard Thomas: There may be a risk of that, but all I have seen so far is that all the different initiatives are moving in the same direction, are on parallel tracks, if not exactly the same track, and certainly given our very strong central role in this as the guardian of data protection, we are an independent body, we will be very concerned to ensure that all the right lessons are drawn from this incident, and that we speak very loudly in making sure that everybody gets the right message.

David Smith: Perhaps I could just add, I think that is very much how we see it. We at the moment are not in the driving seat, we are looking to see what these other inquiries produce, but we have some very clear questions of our own. Mr Thomas has alluded to those, and you, Chairman, have; how is it possible, how did the system allow a junior official to download so much data? There might be not just a lack of organisational measures, which is one of the requirements of the Data Protection Act, but a lack of technical measures. Data protection was not built into the system apparently in the way it should be. What is the whole cultural approach to security? Is it taken seriously from the top, and does that go down throughout the organisation? So we have these questions. We are expecting them to be answered, but if they are not answered, we will come back and make sure that they are answered. At the end of the day, others have powers, but we have powers, and we will be looking at those reports to see whether it is appropriate to use our powers, which are fairly limited, and we can come on to that, to put recommendations into effect if they are appropriate ones.

Q9 Dr Whitehead: Obviously without prejudice to these various reviews and inquiries, you, I imagine, have a feel for what the rules are, as opposed necessarily to the practice, both in the public sector and the private sector. Does it appear to you that those rules in general for data sharing and exchange, and indeed for transfer, are similar between Government departments and agencies and the private sector, or do there appear to be different levels of practice?

Richard Thomas: The rules are in the Data Protection Act, which comes from the Data Protection Directive. The seventh principle is fairly straightforward, it says that 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. That is the basic requirement to take appropriate security safeguards. It is elaborated in the legislation by a need to have regard to technological development and the cost of implementing measures. Measures must ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, and the nature of the data to be protected. So it is expressed in terms

which means that it recognises that personal data can have different levels of sensitivity, and different consequences can follow from loss or leakage of the information, but we have been, over the years, very keen to set out the guidance. Only in October of this year, before this all came to light, we published a checklist for small and medium-sized organisations. If I can just quote from some of the guidance we put into the public domain in October of this year, we said: "Do your staff know: to keep passwords secure? To lock/log off computers when away from their desks? To dispose of confidential paper waste securely by shredding?" Then it goes on through various other bullet points: "To encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen?" So this was a checklist for small and medium-sized enterprises, and we certainly would anticipate and expect any major public authority to be well beyond needing that sort of advice.

Q10 Dr Whitehead: But with respect to the rules in the legislation, would you perhaps describe those as a little like guidance to prison warders that prisoners should not escape, and that perhaps there should be, in legislation, as opposed to guidance, minimal technical standards for data transfer, password protection, data encryption, perhaps at a legislative level, rather than a guidance level; would that be possible to achieve, or is that perhaps something that sits well elsewhere?
Richard Thomas: Well, there are many British and international standards on security, and the general approach we take is that organisations must follow the appropriate standard for their particular business or organisation. I am reluctant to go down the road of too much prescription in legislation itself, because you have such a vast range of different sorts of situation, but over the years, and David might want to elaborate this, we have given a lot of guidance about the value of these various standards, and encouraging data controllers to follow the particular standard and the changing technology—it is changing all the time—appropriate for their circumstance.
David Smith: I think it is a question of the way in which technology develops. Encryption is, as you know, technology for scrambling data so it cannot be readily accessed, but the techniques for that change all the time. I will not go into the technicalities of 128-bit encryption, but what, if you like, today is entirely secure, in three years' time will be fairly easily broken into, and the technology will have moved on. So to write that and the proper standards into the legislation is extremely difficult. I think we do largely take the right approach by setting out the general principle in the legislation of appropriate security, and then through guidance, and through, I think, businesses, whether it is Government or others, taking responsibility. They do have to look at the sort of data they hold, a risk-based approach, and come up with appropriate measures, working from guidance. I do not think you can take away, if you like, the responsibility, whether it is Government departments or business, for making their own assessments, and applying appropriate security measures.

Q11 Dr Whitehead: But presumably there is a distinction between doing something which nevertheless those people who wish that system ill might have got ahead of the people who are dealing with the data transfer or the data sharing and might attack it, and simple human error/stupidity in doing things. I mean, how can one become rather more like the other in terms of the process, over and above laying down guidelines?
David Smith: As far as possible, the system should not allow human error, so in this example, and again, I am reluctant, without seeing the results of the inquiries, to comment on what has exactly happened, but a junior official should not be able to put in a disk and download data on to a disk. The system should not allow that to happen. There is something wrong if that can happen.

Q12 Dr Whitehead: So that is the combination of, as it were, human error and system error.
David Smith: That is right.
Richard Thomas: The way I put it in the press interviews I did when this became public knowledge, I said "Any system has to be proof against criminals, proof against idiots and proof against those who break the rules". That is, I think, the test we would expect, particularly for a database on this particular scale.

Q13 Chairman: You read out a list of rules, virtually every one has been broken, to our certain knowledge, in some cases with disastrous consequences. You read out earlier a number of rules and principles.
Richard Thomas: We do not have any suggestion in this situation that criminals have been involved. We have other situations—

Q14 Chairman: No, I am talking about rules of procedure which have broken, in terms of not downloading on to separate disks, in terms of not leaving computers logged on when you are away from your desk; all rules which we see broken week in, week out, do we not?
Richard Thomas: We do not know exactly what happened here, Chairman, I am reluctant to be drawn—

Q15 Chairman: I am talking more generally.
Richard Thomas: More generally, I would not like to condemn all public bodies and all private bodies, I think our experience is that most organisations do take these requirements very seriously, and most, as a matter of self-interest, not just because they have to comply with the law, do try to take these matters seriously. But I think that as technology becomes ever more pervasive, it is ever cheaper and easier to process vast amounts of personal information. I think the point we are making, and making in the annual report, was that the risks are becoming greater all the time. So much personal information is

now being collected and processed that the risk must be ever greater, and perhaps there has been a bit of a tendency to put excessive faith in using technology, using the collection of information, sharing it around, for perfectly understandable reasons—law enforcement, the fight against terrorism, improving public services—perhaps without giving sufficient thought to addressing the risks that go with that collection of information.

Q16 Dr Whitehead: Before all this most recent series of events occurred, the Government had published an Information Sharing Vision Statement, in September of last year, and in that, among other things, they stated: "The existing law ensures that appropriate safeguards will be maintained on the sharing of medical, taxpayer and criminal records information in particular. But within that law, it is possible for there to be greater information sharing than currently occurs -- and this can be combined with proper respect for the individual's privacy." It looks a little dated now, does it, do you think?
Richard Thomas: I think it does, yes. Perhaps it looked a little bit dated when it was published. We noted the Vision Statement from the Ministry of Justice, and we had some reservations about that. We saw it at one stage in draft, and we made some suggestions for improving it, but I think at that time, there was perhaps too much faith in the benefits of information sharing. If I can just read from the introduction to that statement: " . . . the Government is committed to more information sharing between public sector organisations and service providers." It went on to say: "We recognise that the more we share information, the more important it is that people are confident that their personal data is kept safe and secure." But we thought that was perhaps not the end of the story. Since then, we published what we call our Framework Code of Practice for sharing personal information; this is quite a detailed code which we have been urging on public bodies for where they are sharing information, when there is a good reason to do so. Above all, that is the important thing, first of all, to identify why you are collecting and sharing information, and then make sure that you stick within that particular remit. But if you do need to share from one organisation to another, our Framework Code is meant to provide a template for more detailed codes in particular situations. That has a page on the importance of taking security very seriously, and it elaborates the legal requirement which I shared with you earlier. The vision statement, I think, is also a bit dated, because since then, on 25 October, the Prime Minister made his, I think, very important speech on Liberties, and that included some three or four pages on privacy and data protection. I think we welcome the sentiments expressed by the Prime Minister in that speech, and that included the announcement of an independent review to be carried out by myself and Dr Mark Walport, who is the chief executive of the Wellcome Trust, and that is primarily looking at information sharing, recognising the difficulties, the controversies it generates. Our independent review is just now getting underway; the HMRC incident came along only a week or two weeks or so after that was announced, but our review is getting underway, we shall be publishing a consultation paper very shortly indeed. I think that is going to take rather a fresh look, not least in the light of recent events, at the whole question of information sharing.

Q17 Mr Michael: In the first place, could I ask you about one of the specific recommendations of the House of Lords Science and Technology Committee in August? Because they recommended there the introduction of a notification requirement for breaches of data security standards. Would such a requirement have made a significant difference as to how the incident at HMRC was dealt with? Secondly, in what situations do you consider that a notification requirement would be beneficial?
Richard Thomas: I think, Mr Michael, we are now moving on to possible changes to the law. We are not alone in this country in encountering security breaches. There have been a number of incidents, particularly in the United States, and a number of laws have been enacted in I think now the majority of the states requiring some sort of breach notification. Most of the American laws require notification to the individuals concerned. As we said to the House of Lords Select Committee on surveillance issues, we think that prima facie, there is a good case for introducing a breach notification law into this country. I think it is for debate still as to whom you notify, whether it is the individuals who have been affected or the Commissioner responsible for regulation of the market. Our instincts are that it would be wise to include provision for notification both to the individuals and to ourselves, but only on what I might call a discriminatory approach—only in those situations where there has been a substantial risk of damage or distress, because we have to be careful not to get bogged down with trivia.

Q18 Mr Michael: I accept that, I think that is the point of the question really, asking in which circumstances do you think it would be beneficial.
Richard Thomas: Certainly any significant case having a substantial risk of damage or distress. You started by asking whether it would have made a particular difference in this situation. At one level, no, because we were told about it once the politicians knew about it, and as I have explained earlier, they came to see us almost straight away, so we had no complaint on that. But I think it might have made a difference if people were aware that there had to be a notice given to those affected. I think that will serve a very valuable deterrent purpose, and make both organisations, the system, and the individuals, the top, the middle, and the junior, take these matters that much more seriously.

Q19 Mr Michael: So you think it could have a prophylactic effect, and not just—
Richard Thomas: Yes, I put it very much in those terms.

Q20 Mr Michael: Going more widely in terms of what is needed, in the light of the HMRC case, do you think there are changes in the criminal law that you think are necessary? There have been suggestions that, for instance, Government departments or agencies, rather than individual civil servants, should be held criminally responsible for data protection violations. You have submitted proposals for new criminal offences. Could you give us perhaps a brief summary of that? Have you received any feedback from Ministers, particularly in the Ministry of Justice, in relation to those proposals?

Richard Thomas: You are right, Mr Michael, we have put proposals to the Ministry of Justice, and we did this some time before the HMRC event came to light. Indeed, for many years, we have been arguing about the need for increased inspection powers. Perhaps we might return to that one later. More recently, we have been putting the case for stronger sanctions in the form of a new criminal offence, and we have prepared a detailed paper on this. The paper was submitted, I think, in September/October to the MoJ as a draft paper; it is still a draft, because we are still doing a bit of research on the equivalent law in other countries and so on. We are very happy to share that paper with this Committee in its final stage, which I imagine would be in another a couple of weeks or so, we would be happy to share that paper with you, but we are reasonably clear what we are looking for. In the area of new criminal sanctions, what we have put forward in some detail is the need for a new criminal offence which is linked to the existing duty under the Act. Already the Act says: "It shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is data controller." That is already, and has been for many years, a legal duty. That is section 4 of the Data Protection Act. What we are now suggesting is that there should be a new criminal offence linked to that duty, but limited to breaches that are avoidable, those that give rise to a serious data protection risk, and those where a criminal state of mind exists. We have elaborated on this in saying that the offence should be created where a data controller knowingly or recklessly fails to discharge the duty imposed by section 4, and where that failure results in a substantial risk that any person will suffer damage or distress. We then go on to say it should be a defence that the data controller exercised all due diligence to comply with the section. So I hope you will see we are trying to take a balanced approach. We are not just creating criminal offences for the sake of it, we recognise the regulatory burdens which can be excessive, we are looking for a targeted new criminal sanction to serve the prophylactic effect that you already have described, and to, if you like, raise the profile of the importance of complying with these principles, but also to give us a real power to take punitive action in those cases where that is merited.

Q21 Mr Michael: I very much take the point of the need to get a balance into this, because I think it is important to ask you the opposite question, which is not really the thrust of events, and that is: are there dangers of failing to share data that should be shared? I say this because I saw something of this in relation to sharing information for the prevention of crime, for instance, where there was very much a culture, both in local authorities and the police, of lawyers and data protection officers saying, "If in doubt, don't share", rather than, "If in doubt, question again the balance of whether you should or should not; what are the public interest issues?" So is there a danger of getting too defensive a culture because of the shocking events that have woken us up to the need to provide protections?

Richard Thomas: You use the word balance in your question, and balance is at the heart of data protection. We are very much aware that sometimes people have a perverse attitude or interpretation of the law and take a very sort of ultra-cautious approach. And we have been very keen indeed, in the context of information sharing, to make it absolutely clear that the law does not prevent appropriate sharing. What it does do is say: be clear about what you are doing, why you are collecting the information, and why you are sharing it, and then make sure you follow the various procedures and requirements. Very rarely does data protection law completely stop anything happening. What it does do is regulate the way in which things should happen; so if there is to be sharing, it should be properly regulated sharing, it should not be stopped altogether.

Q22 Mr Michael: In relation to those regulations though, I was very taken by the fact that before you went into expressing the dangers against which there should be adequate protection, you said in your annual report, "Although many of the detailed rules are too bureaucratic"; you went on to say that the underlying principles of data protection had successfully stood the test of time. I was taken by that point because although many of the detailed rules are too bureaucratic, it is reinforced by a point in the report, "Better use of personal information", which was the report done by Dr Mark Walport, which says: "The legislative regime is critical to this area, but it is complex and not well understood, in particular the Data Protection Act. Greater clarity is needed urgently: the large amount of guidance, often at a Departmental level, serves simply to confuse." You are asking for clarity; that does require, does it not, a principle-based approach, rather than something that depends entirely on tick box processes for dealing with the issues?

Richard Thomas: I am nodding at virtually all the points you make, because I recognise very much the thrust of what you are saying. The European Directive is a rather strange mix of some principles, which I think are first class, and have stood the test of time very well, but some rather prescriptive requirements which have been largely translated into UK law. As the regulator, it is my job to make sure the law is followed as far as possible, but I have expressed the view in my annual report that some of these are excessively bureaucratic and perhaps too prescriptive, and I recognise that there has been

some negativity towards the data protection legislation over the years. I have been Commissioner five years to the week, and it has been part of my mission to clarify, to simplify, to put as much guidance out as possible. We have now moved, in the last two or three years, to putting out a major series of good practice notes, trying to put in very simple terms the dos and don'ts of data protection. At the heart of our mission, if you like, now for data protection is a statement along the lines, "Our role is to make it easier for the vast majority of organisations which want to take data protection seriously, and are trying to take it seriously, but tougher for the minority who fail to take it seriously". So I recognise what you are saying, we have to get across the fundamental importance of the basic principles, as far as possible appeal to the enlightened self-interest of organisations, give them as much guidance as possible, and at the same time see whether we can, at both European and domestic level, move towards greater simplification of the law itself.

Q23 Mr Michael: That is very helpful. You did touch in your first reply on the question of spot checks of Government departments. What is the current position on unannounced ICO inspections without the consent of the data controller, and are you satisfied with the proposals that the Prime Minister has outlined in terms of inspection powers?
Richard Thomas: We have been dissatisfied for a long time. We are a regulator with very limited powers of inspection. We do have a power to obtain a search warrant, but that is only where we are looking for very hard evidence of some major breach; that is, if you like, a nuclear sanction. Otherwise, we can only assess the compliance of a data controller with the consent of that organisation. I find that a very bizarre situation, unlike virtually all the other data protection authorities around the world, and unlike most of the regulatory bodies in this country, Health and Safety, Financial Services, Food Standards and so on. So we have been arguing for many years that we need the power to carry out an inspection on any data controller without having to get the consent in the first place. As part of the paper I mentioned earlier, we yet again set out in some detail the powers that we would like. We have put a very detailed case forward, and we have modelled that on section 54A of the Data Protection Act, which somewhat ironically does give us the power to carry out an inspection for certain international organisations. David is my great expert on this, and will elaborate in more detail. We do have the power to inspect certain international organisations, but we do not have the power to inspect any public, private or voluntary sector organisation inside the UK. So that is essentially the change in the law which we have been seeking.

Q24 Chairman: How does that come about?
David Smith: It comes from a number of international conventions, in particular the Europol convention. When Europol, the European Police Office, was set up, it took the typical European model of data protection rules, which is an ability for the supervisory authority to conduct inspections without consent. Because each Member State inputs data, at each Member State's level, that power to inspect has to be given to the local supervisory authority. So under the Europol convention, the UK has to give us, as the UK data protection authority, a power to inspect Europol data in the UK. So we have that power for Europol, for Schengen, when the UK joins Schengen, for the customs information system, but not domestically for UK data. So we really say just take that same power and extend it across the board.

Q25 Chairman: Are you going to get the power?
Richard Thomas: Well, if I can just continue with the answer to Mr Michael's question, the Prime Minister announced that we will, if you like, de facto have the power to carry out spot checks inside Government departments, and I understand that is going to be achieved by an instruction to Government departments to let us in, to give us consent. So that is, you know, de facto for the time being, but in my conversations with the Secretary of State and with his officials, I have made it very clear that we are looking for the statutory power not just for Government departments but right across the piece. We do have some optimism that the power is going to be granted. There is going to be a Governance of Britain Bill later in this session of Parliament, and I think we would be hoping that that Bill will include an amendment of the Data Protection Act to give us that power of inspection without consent. It has been an anomaly, in my view, for many, many years, it does not make sense. I think it does reflect, and this is a wider question, perhaps that data protection has not been taken with sufficient seriousness by successive governments. In answer to your question, also, I would say, I remain dissatisfied, because we cannot do these inspections without adequate resources. We cannot even do spot checks of Government departments on a de facto basis without the resources to do it. We have to provide the entire data protection activities of my office on a budget of £10 million a year. If I compare that to the Health and Safety Executive, £890 million a year; the Financial Services Authority, £269 million a year; Food Standards Agency, £143 million a year. This is just from some quick research over the weekend. £10 million is the entire budget for data protection, none of which comes from the Government, it all comes from the notification fees from data controllers. This Committee is aware that the Freedom of Information budget is even smaller, that this year stands at £4.7 million, and that is grant in aid from Government. Maybe that is another story.
Chairman: I think Mrs Morgan wants to ask you questions in this very area.

Q26 Mrs Morgan: Yes, indeed, but before I go on to that, I want to ask you about enforcement powers. I think in your evidence to the Home Affairs Select Committee you lamented your lack of any real teeth

in this field. Currently, I understand you can only issue enforcement notices and prosecute individuals or private organisations for certain breaches of data protection laws. So would the introduction of a power to issue fines or fixed penalty notices benefit your work, do you think?

Richard Thomas: Well, Mrs Morgan, what I was saying earlier about the need for a new criminal sanction would go a long way to address the deficiencies in the existing law. At the moment, we have the power to serve an enforcement notice, but if I can paraphrase the law, an enforcement notice says, "You have got it wrong, do not do it again", and only if they do it again, in explicit breach of our enforcement notice, only then is it a criminal offence. That is a long drawn-out process which, going back to the earlier metaphor, involves bolting doors after horses have disappeared. So yes, we would like to see a new criminal sanction. Once that is in place, then one might go on to look at a power to impose a civil penalty. There is legislation going through the House at the moment, the Sanctions and Redress Bill, which allows regulators in certain situations to impose a fixed penalty instead of taking a criminal prosecution, but I think that may follow from that particular development. I have mentioned also the possibility of a notification duty. Another couple of suggestions I would like to share with the Committee if I may: one is that we think there is considerable merit in our—as the regulator—having the power to require an organisation to commission its own independent review of a particular activity. This will be, if you like, in parallel to inspections which we ourselves carry out, or inspections which we carry out but we outsource to security experts or other people who can really get into the heart of a particular system. But the third element would be a power for us to require an organisation to commission an independent report. This is, if you like, part of the modern regulatory agenda; other regulators have a similar power. The final suggestion we would like to share with you this afternoon is that there might be some sort of reporting duty on certainly major organisations, public and private, to include in their annual report some sort of confirmation that the person signing off the report, whether it is the Minister or the Permanent Secretary or the chief executive, is satisfied that appropriate security safeguards have indeed been put in place. That is something this Committee may like to consider, we could elaborate on that if you would like us to.

Q27 Mrs Morgan: Right, thank you. I think that is sufficient there. I wanted to go back now to the funding issue, because you very graphically described your position with regard to funding, and used other organisations as examples of much higher funding. You have talked about your extremely limited resources, and we know the problem with the Freedom of Information part of your work. Are you satisfied with the Government funding which you receive to carry out your data protection work?

Richard Thomas: We have to keep our two revenue streams quite separate. We have a revenue stream for data protection which comes through the fees that we receive, and that is about £10 million a year. Then Freedom of Information is funded quite separately by grant in aid from the Government. Starting with data protection, that would need to be increased quite substantially if we are to take on a serious inspection role. I have made it clear that even the spot checks of Government departments we could not do without some resource. We cannot conjure those resources from nowhere. So there would have to be an increase just to do that in the short term. But looking to the medium and longer term, if we are to have what I would call sensible and adequate inspection powers, then we would need to have resources to do that. There is a discussion which we have already started to have with the Ministry of Justice about how that might be achieved. There are three basic ways: the first is to increase the fees, whether for all data controllers or on a more discriminating selective basis; the second would be grant in aid for data protection activities; and the third would be to charge a service. We are entitled, under the Act, to charge for a service, so one could go in and carry out an inspection of an organisation and say, "Well, we will charge you for carrying out that particular inspection", and I think the debate is still going on as to which would be the most appropriate way forward.

Q28 Mrs Morgan: Which do you think would be the most appropriate way?

Richard Thomas: I think in the longer term the fee income really has to be the right way forward. Whether it is a flat increase for all data controllers or a more discriminating approach, charging more for the larger organisations on a sliding scale, we are still looking at the detail of that. I think that must be the right way forward on a statutory basis. But for the very short term, to carry out non-statutory spot checks, this requires the consent of the Secretary of State, but if he agrees, then charging each Government department for each inspection may be the best way forward. Going right back to some of the earlier questions about all the various reviews going on, we would expect the review being led by the Cabinet Secretary to inform which department we look at first; we obviously take a risk-based approach, and we go into those departments where there is the greatest need.

Q29 Chairman: Mr Thomas, did you say earlier that Government data controllers contribute from their departments, so are they contributing on the same basis as the private sector?

Richard Thomas: At the moment, every data controller pays £35, so the Home Office or the Treasury—

Q30 Chairman: Revenue & Customs pay £35?

Richard Thomas: Revenue & Customs pay £35, as does the sweet shop around the corner.

Q31 Mr Michael: Or the average MP.
Richard Thomas: It is a bargain at the price.

Q32 Chairman: That is a patently absurd situation.
Richard Thomas: Yes, but it does have the huge advantage to us that it is very simple to administer.

Q33 Chairman: £1 each would be simple to administer.
Richard Thomas: You could base it on turnover, number of staff, other ways, but there are complications in all of those. This does have the great benefit of keeping it pretty low for all those who contribute, but I recognise there are some inherent unfairnesses in the current arrangements. In the longer term, I certainly think that fees must be the right way forward. We have been exploring various models, and we could have some very substantial fees charged to some very substantial organisations, and very low fees to everybody else.

Q34 Mrs Morgan: I understand that in your own department, a new pay system is being introduced, and there is some concern from staff, and the PCS Union are balloting for the staff's view. I wondered if you had any comment on that, and obviously, as you are such a pressurised department, how are you going to cope if staff are concerned and upset about these proposals?
Richard Thomas: Could I start by finishing my answer to your previous question, which was: "Are we satisfied with funding?" and I had made it very clear the grant aid for Freedom of Information is not proving sufficient. After three years, we are moving now into more of a steady—

Q35 Chairman: We will turn again to Freedom of Information.
Richard Thomas: We may come back to that, but that just conditions our level of resource generally. The level of pay for our staff has been a long-running difficulty. I shared views with this Committee some three years ago about the very considerable difficulties that we experience. The pay which we are able to pay to our staff has been quite significantly below market comparables for this sort of work. We have been engaged in some very difficult discussions with the Ministry of Justice. The law says that we cannot pay anything to our staff without the consent of the Ministry of Justice, or the Secretary of State, and that in turn requires the agreement of the Treasury. This has been a saga running now for at least three years. We have reached an agreement with the Ministry of Justice that we can increase the pay of our staff on a three-year settlement, and that was shared with our staff some three or four weeks ago. For the first year of that, that will be at the top end of public sector pay settlements, so there will be some catching up with comparables elsewhere. It is a settlement for the first year just below 4%, and with equivalent changes going on for the second and third year of that settlement. It has various attributes associated with it, namely a move away from automatic progression through a pay scale to a reward system which is based more on the fulfilment of various explicit competencies. We are asking our staff to work very hard indeed, and we have a very loyal and very committed workforce, but it is no secret inside and outside the organisation that they are less than satisfied with the pay settlement put forward.

Q36 Mrs Morgan: So this is sort of performance-related pay, is it?
Richard Thomas: No, it is not performance-related pay. Sometimes it is viewed in that way, but it is not pay in any way which is linked to the fulfilment of personal or organisational targets, it is pay which is linked to displaying certain behavioural and other competencies, technical and other competencies, but it is not performance-related pay.

Q37 Mrs Morgan: But obviously you are aware of the unhappiness of your staff?
Richard Thomas: Yes, I think it has been a very difficult situation. We have a very loyal staff, and we have quite low levels of turnover. No one comes to work for our organisation for the money, they do it because they believe very much in the work which we have to do, and I find myself in an uncomfortable position saying to my staff, "This is the best possible deal we could have secured in the circumstances, but I recognise it is not going to be particularly attractive".

Q38 Mrs Morgan: So you do not think there is any chance of improving that deal?
Richard Thomas: We are still in discussion with the trade unions, but the Ministry of Justice has made it clear to us that in terms of the financial aspects, that is as far as we will be able to go this time round.

Q39 Chairman: It is not coming out of their budget.
Richard Thomas: Well, the grant in aid is coming out of their budget, for Freedom of Information, and we have to have the same pay regime across the entire organisation.
Chairman: Dr Palmer?

Q40 Dr Palmer: I have got a couple of questions about the Identity Card Act. Before we come to that, just returning for a moment to the HMRC scandal, public tension has focused very much on the volume of data, this 25 million. Would you agree that in many ways it is actually the nature of the data which is the more critical issue, because if 25 million anonymized records had been lost that would have been very disturbing but would not particularly have affected most people, whereas even if 10,000 names, addresses and child benefit records had been disclosed, that would have been very worrying for 10,000 people?
Mr Thomas: I agree entirely with what you are saying. I think, quite apart from the volume, it was the nature and the extent of the information. This was names, addresses, details of children, national insurance number, bank sort code, bank account number. It is that combination of information, that availability, which makes it particularly worrying if this data were ever to fall into the wrong hands. I

think we all pray and hope that it is sitting at the back of a rubbish dump somewhere, frankly, but, if it were to fall into the wrong hands, then the implications would be very serious indeed. I mentioned earlier that we have had number of organisations coming to us with confessions of data breaches, but so far all appear to be substantially less serious. In one example a hard disc had gone missing but it only had names and addresses and it was encrypted, and that did not seem to me to be a particularly serious matter, not on the same scale as HMRC.

Mr Smith: If I might just add, Chairman, this adds to the questions which we want these inquiries to look at very carefully. It is not just the security aspect, but why were these data going from HMRC to the National Audit Office and why was such an extensive data set being carried across? We have read some things in the press, which are extremely worrying, about the approach to that, and we do not know until the inquiry comes out, but there are questions for the National Audit Office in this as well as for HMRC. Data minimisation, keeping the amount of data that is kept and what is passed across from one organisation to another, is absolutely key to data protection and, when we are talking about these technological approaches, we are not just talking about security, we want a technological approach to the whole of data protection, what we term privacy enhancing technology: building in compliance, data minimisation, checks on accuracy, all part of the system, Chairman.

Q41 Dr Palmer: I worked in IT for nearly 20 years and my experience is that IT staff will always look for a way round to make life simple and provide the information quickly if they can. So, unless otherwise instructed, they will tend to send the whole database rather than be selective. Would you agree that actually, other things being equal, it might be a good rule for government, indeed for data holders in general, to anonymize data unless there is a good reason not to do so?

Mr Smith: I can say no more than, yes, it would. It would be more than a good thing. I think data protection requires that. If you do not need identifiable data, you should not be using it. Keep what you have, the identifiability and the sensitive information, to an absolute minimum, because the more there is the greater our concerns and it is these large collections that do bring vulnerability with them.

Q42 Dr Palmer: That brings me to my next point. I do not want to put words in your mouth, but reading your submission on the ID Card Bill when it first appeared, the two major objections which I think you were putting forward: one was the audit trail and the other was the retention of secondary data relating to identity after the identity had been proved. To take an example, if somebody has a work permit to work in this country, once it had been verified that it is indeed him and he has got this work permit, you question: "Do we still need to have the work permit data inside this database?" Is that a fair summary of the two points?

Mr Thomas: I think the major point we are making is that any massive collation of information like this carries risk, and our whole approach, if you like, is to either avoid the risk in the first place or to minimise the risk. Certainly we had very strong anxieties and continue to have strong anxieties. You call it the audit trail. I think actually we call it more the data trail. Yes, there can be a good case for having certain arrangements for audit to make sure that the system is being used properly, but we continue to question why the identity card system needs to collect transactional data. One might be able to envisage a scheme where you issue the card and some basic details are checked at the time the card is issued, but we are even more concerned about the record of the card being used every time: every time you pass through Heathrow Airport, every time you use it in connection with public services. We do not know exactly, because I think the Home Office or the Passport and Identity Agency is still elaborating which way it wants to go in this area—I think there is still a lot of debate to be had about the future of identity cards—and I am sure that this recent incident will cause even more searching questions to be asked. But we still, I think, have some uncertainty about what are the primary functions, what are the primary purposes, of the identity card. It is only when you understand what it is really there for that you can then say how much information needs to be collected. Is it to improve policing? Is it the fight against terrorism? Is it to improve public services? Is it to avoid identity theft? Is it to allow people to prove their identity? I think there is a lot of thinking still to be done as to what the primary purpose is. There are still reports to be published. There is a report by Sir James Crosby on identity management which has not yet been published. I think the future still needs to be discussed. David was saying earlier, data minimisation is a key principle associated with data protection and keeping this massive database with records of every time the card is swiped through a terminal would be distinctly unattractive and would, I think, increase the risks which might occur. The retention issue is a separate one. I do not think it has been top of our list of concerns but it is one of our concerns. Clearly, data protection says do not retain any information longer than you need it and, if you need some information, just to verify identity at the point of issue and then, unless there is very good reason, you should not retain that indefinitely subsequently.

Q43 Dr Palmer: With my former IT hat on, I was not struck in this debate by the emphasis given to having the data on a single database as opposed to several databases. It always seemed to me that this is a slightly 1970s approach in that the idea at that stage was that if you had access to a database you had access to all the fields in it. I wonder whether we should not be looking more at the software protection of individual data fields. To go back to

the example of the work permit, I cannot see any reason why somebody accessing the identity card database to see whether you are entitled to a pension should also have a legitimate reason to look at your work permit. Would you not agree—I put it in short to you—that actually the key issue is not so much whether it is in one database, or two databases, or five databases, but whether people have access to the databases and whether they have access to the fields in those databases, because as a former programmer, if I have got the access, I have got the right to look at it, then I can very easily link the five databases together.

Mr Thomas: I think some of those questions, Dr Palmer, are more appropriate for those running the particular system, in this case the Identity and Passport Agency. The general thrust of what you are saying I agree with. The Government has announced that it will no longer create a single new database for identity cards; it is now saying that biographic data will be kept on the DWP customer information system, that biometric data will go on an existing IND system and that the use of the cards will go on a PKI system. I am not sure. They argue that this separation enhances security, but a mix of new and legacy systems also poses other risks. Will they have common standards between one system to another, what will be the access arrangements and how will this work in practice? I think there are some very searching questions to be asked there.

Q44 Dr Palmer: You do not necessarily feel that it is helpful to split into three databases; it might be helpful, it might not.

Mr Thomas: No, there is a further risk, of course, that you may not have your data as clean as you would like it, and one of the merits of a new database is that you hopefully can start with clean data. The private sector over the years has learned the cost and the difficulty of data cleansing exercises, but if you are starting with existing databases then you are running a risk that you have got already out of date or inaccurate information right from day one.

Q45 Dr Palmer: An entirely separate question on the same area. You will be familiar with the Stork Project at European Union level which, as I understand it, essentially reflects the freedom of movement within the European Union to enable each country to see who it is that is actually coming in and potentially also access their medical or social security data. Do you feel that is a legitimate objective that we should know who is coming in and other people should know who is coming from Britain, and, if so, do you have concerns about the way it is being done?

Mr Thomas: We do not have a huge amount of knowledge or involvement with the Stork Project. That is one of many initiatives here in this area. I think the Stork Project is concerned with migration and movement inside the European Union to ensure better integration or intra-operability of the various systems for recognising identity electronically and I think already there are some tensions between trying to do that and giving maximum autonomy to each Member State. I think those involved with that are still trying to find a way through. I think the Stork Project was announced four or five years ago with a target of intra-operability for the year 2010. That is approaching quite fast now and I do not know quite whether that is going to be achieved or not. There is also the e-borders programme, which is a larger initiative. There was to be a code of practice on that where we were asked for our comments on that, but we had quite a number of comments and we are still making some, and that has not now been published. So, perhaps the HMRC incident has meant there has been some delay in bringing that forward, but it gives us a further chance to make comments on that.

Q46 Mr Sharma: Gordon Brown's recent speech on Liberty is considered to be the turning point in the Government's approach. What is your reaction to the Prime Minister's announcement and what are the great challenges the ICO now faces in terms of its FOI work?

Mr Thomas: I do not wish to make any party point here, obviously, but I was delighted with the Prime Minister's speech. We had been hoping for a speech of that nature for a long time on both data protection and Freedom of Information, because both data protection and FOI are very much about cultural issues. I think everyone recognises that culture is led and changed from the top of any organisation and you cannot get much higher that a Prime Minister. To have a Prime Minister reinforce in some very forthright language the messages on Freedom of Information is very welcome. He called it a "landmark piece of legislation". He said "there is more we can to change the culture and make the workings of government more open". "We should have the freest possible flow of information between government and the people". Public information does not belong to Government; it belongs to the public, on whose behalf government is conducted". So, on Freedom of Information, five pages of that speech were devoted to general messages to take FOI seriously right across the public sector culture and some specific initiatives: the abandonment, in line with this Committee's recommendation, of the changes on fees; the review of the 30 Year Rule and also possible extension of the Act to private bodies exercising public functions. So, we welcome the generality and the specifics. On data protection, the Prime Minister also had some very strong words in support of the principles of taking privacy and data protection seriously. He recognised the value of information for law enforcement and improving public services, as I do, but he went on to say that we must ensure that we retain the trust and confidence of people; that we have to take data protection concerns very seriously. He called this the "Century of Information", which is a nice phrase, and he says that we risk losing people's trust, which is fundamental to all these issues and more.

Q47 Chairman: He did not take long to prove that, did he?

Mr Thomas: I am sure he had no inside knowledge of what was happening inside HMRC. There is no suggestion that on 25 October he had any inside knowledge, but I think, how can I put it, ironically the events of the last couple of weeks have really added force to what he was saying there. And, of course, it was in the course of that speech, Mr Sharma, that he announced the independent review of information sharing, which he has asked me and Dr Walpole to carry out, and we will be doing that over the next six months.

Q48 Chairman: Mr Sharma also pressed you about whether you faced more challenges on the FOI side in the new situation.

Mr Thomas: On Freedom of Information, it has been a very challenging first three years, very satisfying and rewarding but very challenging. In the first three years we estimate there have been at least 200,000 requests made to public bodies and possibly as high as 300,000. Of those about 7,000 have resulted in complaints to my office. We have closed about 6,000 cases and we have made about 740 formal decision notices. So we have been a very busy organisation. We are doing all this on our budget this year of £4.7 million, which I have indicated earlier is simply not sufficient. Now we are approaching a steady state, the volumes have been much higher than anyone expected and the Ministry of Justice has recognised, if cases are taking too long, which I believe they are, it is because of the volume, and we are now working at maximum efficiency and effectiveness. We have put in a substantial bid for increased resources for next year, a very substantial bid, and that is currently being discussed between ourselves and the Ministry of Justice. I would like, if I may, if we are talking about the success of Freedom of Information, to share with this Committee some research we are going to publish in the next couple of weeks, a sort of sneak preview of some of our research. Every year we ask a cross-section of the public, a thousand people, about the benefits of Freedom of Information. It is a longitudinal study. We ask them about the benefits of being able to access information held by public authorities, and we break it down into increasing knowledge of what public bodies do, promoting accountability and transparency, increasing confidence in public authorities and increasing trust in public authorities and, asking exactly the same question. From 2004, 2005, 2006, to 2007, we have seen a massive jump in public awareness of the benefits. In 2004, to all those benefits, the figures were about 54, 53, 51%. Now, for all those, it is 86, 81, 81 72%—so a massive jump—and you can see it rising up on a steady curve through those four years. So I think Freedom of Information has resonated with the public. They have made their requests, they understand the purpose and the importance of Freedom of Information (and, although we have had our difficulties we are still taking longer than I would like to handle some of the cases) I think, as the Prime Minister's speech recognised, it is very much here to stay.

Q49 Chairman: Mr Thomas, Mr Smith, thank you very much indeed. That is a very encouraging note on which to end and we look forward to being touch with you again in the future and hearing further evidence from you as the occasion arises. Good luck in your negotiations of various kinds with the Department of Justice.

Mr Thomas: Would you like us to send the paper to you on powers and sanctions?

Chairman: Yes, that would be very helpful.

Additional information submitted by the Office of the Information Commissioner

The following table summarises more clearly the ICO's FOI research which was mentioned in response to Q48.

ICO Public Survey 2007*

Benefits of being able to access information held by public authorities				
Prompted	**2004**	**2005**	**2006**	**2007**
Increases knowledge of what public authorities do	54%	62%	76%	86%
Promotes accountability and transparency	53%	58%	74%	81%
Increases confidence in public authorities	51%	55%	72%	81%
Increases trust in public authorities	51%	57%	69%	72%

* 2007 Annual track research: individuals

We thought the Committee might like to have the following summary of the improvements we are currently suggesting to the regulation of data protection:

- Power (modelled on section 54A of the Act) for the Information Commissioner to inspect personal data and the circumstances surrounding its processing in order to assess compliance.
- Power for the Information Commissioner to require a data controller to commission an independent audit of specified aspects of its processing personal data.
- Requirement for specified data controllers to confirm in their Annual Report that they are satisfied that appropriate security safeguards are in place. This should be linked to the 7th Data Protection Principle (technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data).
- A requirement for a data controller to notify the Information Commissioner and those individuals affected where a security breach carries a real and substantial risk of causing significant damage or distress to data subjects.
- A new criminal offence where a data controller knowingly or recklessly fails to discharge the duty to comply with a Data Protection Principle where that failure results in a real and substantial risk that any person will suffer damage or distress. There should be a defence that the data controller exercised all due diligence to comply with the section.
- The wider use of Privacy Impact Assessments. (We were unable to mention this concept in our evidence, but we are launching detailed proposals at our conference in Manchester tomorrow.)

Richard Thomas
Information Commissioner

10 December 2007

Printed in the United Kingdom by The Stationery Office Limited
1/2008 386353 19585