



House of Commons
Justice Committee

Referral fees and the theft of personal data: evidence from the Information Commissioner

Ninth Report of Session 2010–12

*Report, together with formal minutes and oral
evidence*

*Ordered by the House of Commons
to be printed 18 October 2011*

HC 1473
Published on 27 October 2011
by authority of the House of Commons
London: The Stationery Office Limited
£8.50

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 Sir Alan Beith (*Liberal Democrat, Berwick-upon-Tweed*) (Chair)

Mr Robert Buckland (*Conservative, South Swindon*)

Jeremy Corbyn (*Labour, Islington North*)

Christopher Evans (*Labour/Co-operative, Islwyn*)

Mrs Helen Grant (*Conservative, Maidstone and The Weald*)

Ben Gummer (*Conservative, Ipswich*)

Rt Hon Elfyn Llwyd (*Plaid Cymru, Dwyfor Meirionnydd*)

Claire Perry (*Conservative, Devizes*)

Yasmin Qureshi (*Labour, Bolton South East*)

Mrs Linda Riordan (*Labour/Co-operative, Halifax*)

Elizabeth Truss (*Conservative, South West Norfolk*)

Karl Turner (*Labour, Kingston upon Hull East*)

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

Jessica Lee (*Conservative, Erewash*); Anna Soubry (*Conservative, Broxtowe*); and Mrs Siân James (*Labour, Swansea East*).

Powers

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

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the internet at www.parliament.uk/justicecttee. A list of Reports of the Committee in the present Parliament is at the back of this volume.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some or all written evidence are available in a printed volume. Additional written evidence may be published on the internet only.

Committee staff

The current staff of the Committee are Tom Goldsmith (Clerk), Hannah Stewart (Committee Legal Specialist), John-Paul Flaherty (Inquiry Manager), Ana Ferreira (Senior Committee Assistant), Sonia Draper (Committee Assistant), Henry Ayi-Hyde (Committee Support Assistant), and Nick Davies (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

Contents

Report	<i>Page</i>
Summary	3
Referral fees and the theft of personal data: evidence from the Information Commissioner	4
Custodial Penalties for breaches of the Data Protection Act	4
Referral fees	6
Lack of power to compel audits	7
Status of the Information Commissioner	8
Conclusions and recommendations	10
Appendix—Letter of 22 September, from Rt Hon Lord McNally, Minister of State, Ministry of Justice	11
Formal Minutes	15
Witness	16
List of Reports from the Committee during the current Parliament	16

Summary

On 13 September we held an oral evidence session with Mr Christopher Graham, the Information Commissioner. The evidence session raised important issues about the protection of personal data, which we address in this Report.

Firstly, we share the Information Commissioner's concern and dissatisfaction that no order has been brought before Parliament to implement section 77 of the Criminal Justice and Immigration Act 2008, which would have the effect of providing custodial sentences for breaches of section 55 of the Data Protection Act. Currently the only available penalty is a fine, which we feel is inadequate in cases where people have been endangered by the data disclosed, or where the intrusion or disclosure was particularly traumatic for the victim, or where there is no deterrent because the financial gain resulting from the crime far exceeds the possible penalty. We accept the Information Commissioner's argument that the issue of custodial sentences for section 55 offences is not exclusively, or even primarily, an issue relating to the media and that the issue should be dealt with by Parliament without waiting for the outcome of Lord Justice Leveson's inquiry (as the Government has indicated is its preferred approach). We urge the Government to exercise its power to provide for custodial sentences without delay.

Secondly, we welcome the Government's commitment to ban referral fees. We do not believe the ban should be limited to personal injury cases. Referral fees reward a range of illegal behaviour, and banning them, together with introducing custodial sentences for breaches of the Data Protection Act, would have the twin effect of both increasing the deterrent and reducing the financial incentives for these offences.

Thirdly, we look at the Information Commissioner's powers. The Information Commissioner offers free data protection audits, but currently a significant percentage of organisations decline his offer. In the wake of the controversy over referral fees, it is noteworthy that no insurance companies have agreed to an audit. The Information Commissioner only has the power to compel audits of a very limited range of organisations, and we agree with him that this is constricting his power to investigate. We call on the Ministry of Justice to work with the Information Commissioner to improve the current system.

Finally, we re-iterate the view of this Committee and its predecessors that the Information Commissioner should become directly responsible to, and funded by, Parliament.

Referral fees and the theft of personal data: evidence from the Information Commissioner

1. On 13 September we held an oral evidence session with Mr Christopher Graham, the Information Commissioner. A number of important and timely issues were raised, to which we would like to draw the attention of the House. We also asked the Ministry of Justice (MoJ) for a written response to the Information Commissioner's comments, which is published with this Report.

Custodial Penalties for breaches of the Data Protection Act

2. The Data Protection Act 1998 (DPA) gives people the right to know what information is held about them and to correct information which is wrong. The DPA also protects the interests of individuals by obliging organisations to manage the personal information they hold in an appropriate way. Section 55 of the Act makes the knowing or reckless obtaining, disclosing or procuring the disclosure to another person of personal data a criminal offence. Section 77 of the Criminal Justice and Immigration Act 2008 gave the Secretary of State power to make an order (subject to affirmative resolution) to introduce custodial sentences of up to two years for section 55 offences. Section 77 of the 2008 Act has been commenced, but the order-making power has not been used. Section 78 of the Act (which has not been commenced) would introduce a public interest defence for section 55 offences.

3. The DPA sets out the current penalties for breaches of section 55 offences. A fine of up to £5,000 may be imposed in the magistrates' court, or an unlimited fine in the crown court. However, in practice fines are much lower, in part because judges and magistrates must take into account the defendant's ability to pay.¹ The Information Commissioner's 2006 report *What Price Privacy?* included details of 26 criminal cases, in which all of those involved received a fine and/or conditional discharge. The highest fine was £1,000 per offence, but some fines were as low as £50 per offence.² More recent cases have seen fines of £100–£150 per offence.³

4. Mr Graham drew to our attention several problems with the current level of penalties. The first is that breaching the DPA can be extremely profitable. In one case a nurse was providing patient details to her partner who worked for an accident management company. A fine was imposed of £150 per offence, but accident management companies pay up to £900 for one client's details.⁴ The Information Commissioner's 2006 report estimated that people were charging around £750 per "mobile telephone account enquiry", and £500 for an unauthorised criminal records check, far more than they are likely to be

1 Q 3

2 *What price privacy? The unlawful trade in confidential personal information*, HC 1056, 2006

3 Q 1

4 Q 22

fined even if caught.⁵ The second issue concerns cases which might not have a financial motivation, but where the potential or actual impact of the crime is severe. A woman whose husband had been jailed for sexual assault accessed the bank account details of the victim. The woman attempted to monitor the victim's spending and social activities but was only fined £100 per offence.⁶ In 2008, two former members of the BNP posted the party membership list on the internet. The district judge at Nottingham Magistrates' Court said: "It came as a surprise to me, as it will to many members of the party, that to do something as foolish and criminally dangerous as you did will only incur a financial penalty."⁷

5. Mr Graham told us that the Government was looking at doing more, including seeking restitution under the Proceeds of Crime Act 2002, and investigating making section 55 offences recordable offences.⁸ However, he did not feel that this was enough:

It just beggars belief that, when more and more organisations have a right to our personal information, to access and process it, the courts do not have the full range of potential sentences to deal with an offence which can involve any of us. This is not about celebrities' hospital appointments. This has the potential to wreck people's lives. Parliament cannot just sit back and watch this sort of thing happen.⁹

6. Mr Graham also told us that he was worried that the issue of custodial sentences would be "caught up in the reeds" of Lord Justice Leveson's inquiry into the culture, practices and ethics of the press. Lord Justice Leveson aims to publish his initial report in the "broad timeframe" of July 2012.¹⁰ However, Mr Graham argued that: "[Parliament] cannot subcontract that to a High Court judge. Sections 77 and 78 of the 2008 Criminal Justice and Immigration Act are there to be commenced, and it is in your power to do that."¹¹

7. The MoJ told us in its written submission that in many cases section 55 offences were committed in conjunction with other offences which already carry custodial sentences. These include telephone and computer hacking, fraud (which can include pretending to be someone else in order to gain access to information for financial gain), bribery, misfeasance or misconduct in a public office, and perverting the course of justice. The MoJ also said that, while it recognises that section 55 offences "are by no means limited to the media", it anticipates that Lord Justice Leveson may well want to look at the issue. It intends to wait for his recommendations before deciding what action to take.¹²

8. It is clear to us that the current penalties for section 55 offences are inadequate. If people can make more money from a single offence than the fine which would be imposed for such an offence, then there is no deterrent. There are also cases where people have been

5 *What price privacy? The unlawful trade in confidential personal information*, HC 1056, 2006

6 Q 1

7 http://www.ico.gov.uk/news/latest_news/2011/cashier-spied-on-sex-attack-victims-bank-records-13092011.aspx

8 Q 3

9 Q 1

10 <http://www.levesoninquiry.org.uk/opening-remarks/>

11 Q 1

12 Appendix, p 11

endangered by the data disclosed, or where the intrusion or disclosure was particularly traumatic for the victim, and a fine is not an adequate sentence. The MoJ has drawn our attention to the fact that many section 55 offences are committed in conjunction with offences which do carry custodial sentences. However, we believe that Section 55 offences can by themselves be serious enough to warrant a custodial sentence.

9. We accept the Information Commissioner’s argument that the issue of custodial sentences for section 55 offences is not exclusively, or even primarily, an issue relating to the media and that the issue should be dealt with by Parliament without waiting for the outcome of Lord Justice Leveson’s inquiry. We urge the Government to exercise its power to provide for custodial sentences without further delay.

Referral fees

10. Parliamentary and media activity has recently highlighted the practice of various organisations, including car insurers, police, towing companies, garages, hospitals, and accident management companies in supplying data to personal injury lawyers.¹³ This may be legal if the subject gives their consent, but if they have not done so it is likely to constitute a breach of section 55 of the DPA. Personal injury lawyers will pay a referral fee of up to £900 for each case they receive. Paying such large referral fees drives up the cost of personal injury claims, and is a powerful incentive for organisations (or individuals) to pass on information without permission.

11. Mr Graham told us that even in cases where insurance companies had a clause in the small print of policies giving them permission to pass data to lawyers the practice might still not be legal:

Potentially it is a breach of the first data protection principle. It is not fair processing if you claim consent and all your policy holders say, “I don’t know what you’re talking about—I never knew.”¹⁴

12. During the evidence session we were struck by the range of illegal behaviour that referral fees can reward, from individuals stealing data,¹⁵ to companies with contracts or practices which breach the DPA,¹⁶ to the sending of spam text messages to mobile telephones.¹⁷ Clearly a system which makes criminality so profitable needs to be changed.

13. On 9 September the Government announced its intention to ban referral fees. In a written ministerial statement, the Parliamentary Under-Secretary of State, Jonathan Djanogly MP, said:

Alongside the planned reforms to conditional fee agreements, the ban on referral fees will contribute to the Government’s plans to tackle the compensation culture by

13 Eg. Hansard, Tuesday 13 September 2011, col 896; House of Commons Transport Committee, *The cost of motor Insurance*, Fourth Report of Session 2010–12, HC 59; and <http://www.dailymail.co.uk/news/article-2010446/The-cash-crash-conspiracy-The-4-6bn-racket-involving-greedy-lawyers-insurers-thats-sending-YOUR-premiums-sky-high.html>

14 Q 24

15 Q 22

16 Q 24

17 Q 22

discouraging unmeritorious claims and controlling the disproportionate costs of personal injury claims, without denying access to justice.¹⁸

14. We welcome the Government's commitment to ban referral fees and we do not believe the ban should be limited to personal injury cases. We hope that when implementing the ban, the Government will take into account the fact that referral fees reward a range of practices that are already illegal. Banning referral fees, together with custodial sentences for breaches of section 55 of the Data Protection Act, would have the twin effect of both increasing the deterrent and reducing the financial incentives for these offences.

Lack of power to compel audits

15. The Information Commissioner offers free audits to both public and private sector organisations to assess how effectively those organisations handle personal data. If problems are found the Information Commissioner will not impose a financial penalty if the organisation takes the steps he recommends to address them. If the organisation does not want the report published then it is kept confidential. However, the Information Commissioner's audit powers are limited: while central Government departments and a small number of other organisations must accept audits, the vast majority of organisations are free to decline.¹⁹ In practice 29% of public organisations and 81% of private ones declined last year.²⁰

16. The Information Commissioner told us that there had been circumstances where he had been able to negotiate audits²¹ but that his lack of power to compel audits was limiting his ability to investigate:

We are trying to find out from the Association of British Insurers what they have to say about [allegations around referral fees] and frankly they are not being very helpful at the moment. [...] This is where I am frustrated that I do not have the power to inspect. We have invited a number of insurance companies to undergo voluntary auditing and, surprise, surprise, they are not interested.²²

17. He went on to tell us about the concerns he had about data protection in the health service²³ and local government sectors.²⁴ The Commissioner has recently investigated five

18 HC Deb, 9 September 2011, col 32WS

19 Under the amended Privacy and Electronic Communications Regulations the Information Commissioner has limited powers to audit the providers of public electronic communications services. He can also audit public authorities listed under section 41A(2) of the DPA

20 *Information Commissioner's Annual Report and Financial Statements 2010/11: Information is the currency of democracy*, HC 1124

21 Q 11

22 Q 23

23 Q 11

24 Q 9

large data breaches in the health service and found all five organisations in breach of the Data Protection Act.²⁵ He told us that:

The Information Commissioner's Office has always taken the view that there ought to be the power of inspection. If we think there is a problem, I should not need to get a warrant to break the door down. The Information Commissioner, as the data protection authority, should have the right to come in and check on compliance.²⁶

18. The MoJ told us in written evidence that under current legislation the Information Commissioner must make a formal request to the Government for the power to compel audits in additional sectors. The Secretary of State must then conduct a consultation with the sector before legislation is introduced. The Government has not received any such request from the Information Commissioner. The MoJ also said that it agreed with the Information Commissioner that EU proposals on data protection (expected early next year) were likely to address the issue of the powers of Information Commissioners in this respect.

19. We were surprised that the Information Commissioner has not made a formal request to the Government for the power to compel audits in any of the sectors about which he expressed concerns to us. However, we note that the referral fee issue alone has covered a wide range of sectors. The processes of applying for permission for each sector, with a consultation period for each, undermine his ability to respond in a timely manner to new information. While we are mindful about placing any additional regulatory burden on businesses or public authorities we are concerned that the Information Commissioner's powers are limited in this way. If the Commissioner had been able to compel audits of insurance companies and personal injury lawyers the issues around referral fees might have been identified and tackled sooner. We can see the merits of waiting for the publication of EU proposals in this area, but if those proposals are limited the Government should go further.

20. We are concerned that the Information Commissioner's lack of inspection power is limiting his ability to investigate, identify problems and prevent breaches of the Data Protection Act, particularly in the insurance and healthcare sectors. The audits he offers are free and operate on a risk-based approach and in the last year he has only carried out three or four a month. We call on the MoJ to work with the Information Commissioner to assess how the current system is working, and to consider why he has not formally requested the power to compel audits in any additional sectors and whether this process is unduly cumbersome. Following this the Government should consider the best way to ensure the Commissioner can investigate in a timely manner while minimising the regulatory burden on both the public and private sectors.

Status of the Information Commissioner

21. On 15 September 2011 the MoJ published a Framework Agreement setting out the respective responsibilities of the MoJ and the Information Commissioner. The

25 http://www.ico.gov.uk/news/latest_news/2011/health_service_must_get_it_right_on_data_security_says_ico_0107_2011.aspx

26 Q 11

Parliamentary Under-Secretary of State, Crispin Blunt MP, told the House in a written ministerial statement that:

Under the new framework mechanisms are put in place to enable the [Information Commissioners Office (ICO)] to retain certain types of income, subject to the outcome of the Protection of Freedoms Bill, and the reporting requirements on the ICO are significantly reduced. In addition to this, a number of changes have been introduced to allow the ICO greater freedom to make certain financial and administrative decisions.²⁷

22. He went on to say that the agreement “enhances significantly” the independence of the Information Commissioner.²⁸ When Mr Graham gave evidence to us the agreement had not been published, but it had already been agreed. The Commissioner told us that the Framework Agreement gave him “greater confidence” when dealing with the MoJ but that:

if I am not seen as an officer of Parliament, reporting directly to Parliament, I have to negotiate my way through with many other Departments of State. I have to deal with the Cabinet Office Efficiency and Reform Group controls on marketing activity, which apparently cover the Commissioner’s responsibility to offer advice and guidance. I have to get a tick on anything I propose to do. I am concerned about my website being dragged into some monster Government website, alpha.gov.uk.²⁹

23. Our predecessor Committee, the Constitutional Affairs Committee, first looked at this issue in 2006. It concluded that there was considerable merit in the Information Commissioner becoming directly responsible to, and funded by, Parliament, and it recommended that such a change be considered when an opportunity arose to amend the legislation.³⁰ It revisited the issue again in 2007 when it questioned whether it was appropriate for the MoJ to set the funding levels for the independent regulator and thereby directly influence its capacity to investigate complaints.³¹

24. We welcome the Framework Agreement because it enhances the independence of the Information Commissioner. However, our position is the same as that adopted by our predecessor Committee in 2006, namely that the Information Commissioner should become directly responsible to, and funded by, Parliament.

27 HC Deb, 15 September 2011, col 62-63

28 *Ibid.*

29 Q 27

30 Constitutional Affairs Committee, *Freedom of Information one year on*, Seventh Report of Session, 2005–06, HC 991

31 Constitutional Affairs Committee, *Freedom of Information: Government’s proposals for reform*, Fourth Report of Session 2006–07, HC 415

Conclusions and recommendations

1. We accept the Information Commissioner's argument that the issue of custodial sentences for section 55 offences is not exclusively, or even primarily, an issue relating to the media and that the issue should be dealt with by Parliament without waiting for the outcome of Lord Justice Leveson's inquiry. We urge the Government to exercise its power to provide for custodial sentences without further delay. (Paragraph 9)
2. We welcome the Government's commitment to ban referral fees and we do not believe the ban should be limited to personal injury cases. We hope that when implementing the ban, the Government will take into account the fact that referral fees reward a range of practices that are already illegal. Banning referral fees, together with custodial sentences for breaches of section 55 of the Data Protection Act, would have the twin effect of both increasing the deterrent and reducing the financial incentives for these offences. (Paragraph 14)
3. We are concerned that the Information Commissioner's lack of inspection power is limiting his ability to investigate, identify problems and prevent breaches of the Data Protection Act, particularly in the insurance and healthcare sectors. The audits he offers are free and operate on a risk-based approach and in the last year he has only carried out three or four a month. We call on the MoJ to work with the Information Commissioner to assess how the current system is working, and to consider why he has not formally requested the power to compel audits in any additional sectors and whether this process is unduly cumbersome. Following this the Government should consider the best way to ensure the Commissioner can investigate in a timely manner while minimising the regulatory burden on both the public and private sectors. (Paragraph 20)
4. We welcome the Framework Agreement because it enhances the independence of the Information Commissioner. However, our position is the same as that adopted by our predecessor Committee in 2006, namely that the Information Commissioner should become directly responsible to, and funded by, Parliament. (Paragraph 24)

Appendix—Letter of 22 September, from Rt Hon Lord McNally, Minister of State, Ministry of Justice

The Justice Committee has requested my comments on a number of issues following the Information Commissioner’s oral evidence on Tuesday 13 September. Specifically, you have asked for my views on the introduction of custodial sentences for offences committed under section 55 of the Data Protection Act 1998 (DPA), and the Information Commissioner’s powers to inspect public and private sector organisations. I will cover each in turn, and then provide some further comments on the points raised by the Information Commissioner in his evidence.

Section 55 and custodial sentences

As the Committee will be aware, the previous Government brought forward provisions in the Criminal Justice and Immigration Act 2008 (CJIA) related to section 55 of the DPA. Under section 55 the knowing or reckless obtaining, disclosing or procuring the disclosure of personal data without the consent of the data controller (usually the organisation holding that personal data) is an offence.

Section 77 of the CJIA provides an order making power to introduce custodial sentences for offences relating to the obtaining and disclosure of personal data contained in section 55 of the DPA. Section 77 has been commenced, but the order making power (subject to affirmative resolution) has not been used. Section 78 of the CJIA inserts a new defence for those who can show that they acted for journalistic, artistic or literary purposes, with a view to publication of journalistic, literary or artistic material and in the reasonable belief that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest (this is in addition to the defence already available for those who can demonstrate they were acting in the public interest). This section has yet to be commenced. This Government has said it would keep the matter under review and, as the Deputy Prime Minister said in July, there is a case for looking at this again, and I am grateful for the Information Commissioner’s contribution to this debate.

The Information Commissioner is right to say that section 55 offences and the cases referred to in his predecessor’s 2006 report ‘*What Price Privacy?*’ are by no means limited to the media and the pursuit of celebrities’ personal data; recent prosecutions have shown that this activity can affect those who have never sought to be in the public eye. Nonetheless, this is a matter which we anticipate that Lord Justice Leveson’s Inquiry into the culture, practices and ethics of the press may well want to look at. The Inquiry’s remit specifically includes looking at the media regulatory framework in relation to data protection and why “there was a failure to act on previous warnings about media misconduct”. The media has a well documented interest in this issue, and indeed there is a statutory duty to consult them before making an Order under section 77 of the CJIA. The Government will therefore want to look at what the Leveson Inquiry recommends on these questions before deciding what action to take.

That is not to say that we are disregarding the issue in the meantime. As the Information Commissioner set out to the Committee, there may be other ways of making the illegal trade in personal data less lucrative. For example, under the Proceeds of Crime Act 2002, unlawfully gained assets can be recovered which could be a serious disincentive to trade in personal data. Recently, Orders were made under that Act in the case of two former employees of T-Mobile who had sold customer data in 2008.

It is also important to bear in mind the wider landscape governing of the activity. In many cases, a section 55 offence may be committed as part of a course of criminal conduct which involves the commission of other offences. These might include unlawful interception of communications under Regulation of Investigatory Powers Act 2000 and unauthorised access to computer material under the Computer Misuse Act 1990, both of which carry a two year prison sentence. Under the Fraud Act 2006 it is an offence to dishonestly make a false representation (including as to identity) with a view to financial gain. The maximum sentence is ten years' imprisonment. Bribing another or being bribed is an offence contrary to the Bribery Act 2010. In relation to police officers and other public sector workers, the common law offence of misfeasance or misconduct in public office may also be relevant. All these offences carry custodial sentences. In respect of what the Information Commissioner mentioned about intimidation of witnesses, custodial sentences may be imposed where there are attempts to interfere with jurors or witnesses either under the Criminal Justice and Public Order Act 1994, as contempt of court, or as conduct tending to pervert the course of justice.

Information Commissioner's powers of inspection

In the evidence session, Jeremy Corbyn highlighted the take up of voluntary audits by private sector organisations. The Information Commissioner's power to conduct such consensual audits (often referred to as "Good Practice Assessments") comes from section 51 of the DPA. In terms of non-consensual assessments, the Information Commissioner already has powers to inspect public bodies in this way. Assessment Notices (under section 41A of the DPA) allow the Information Commissioner's Office (ICO) to inspect government departments, or other public bodies designated under section 41A(2), to determine whether or not the data controller has complied or is complying with the data protection principles, regardless of whether the data controller has consented to the assessment.

In relation to the ICO's powers to inspect private sector bodies, there is an order making power in section 41A(9) of the DPA which allows Assessment Notices to be extended to other sectors. However, this power cannot be used without the Information Commissioner making a formal recommendation of the change. The Secretary of State must also conduct a consultation with the sector to be subject to the new power. In considering whether or not to extend the power to a new sector, the Secretary of State and the Information Commissioner must consider the nature and quantity of the data under the control of the new sector, as well as any damage or distress which may be caused by a contravention of the data protection principles by that sector.

The power to serve Assessment Notices under the DPA for private sector bodies is not without precedent. Non-consensual audits of Communications Service Providers (CSPs) in order to determine compliance with the Privacy and Electronic Communications

Regulations 2003 (PECR) have recently been introduced. The Information Commissioner can now audit the measures CSPs have taken to safeguard the security of their services, when previously he could only request that they submit to a voluntary check. Since the power was commenced in May 2011, I am not aware that it has been used.

Ministers have not received a request to designate a sector as liable for Assessment Notices from the Information Commissioner. Should the Information Commissioner request such a designation, I will of course consider consulting on the issue. However, as Christopher Graham pointed out, a new instrument on data protection is currently being considered at EU level, and a proposal is expected from the Commission shortly. I agree with the Information Commissioner that the powers available to him and his counterparts in other Member States, to determine an organisation's compliance with the data protection principles are certain to be considered in this context.

Other data protection matters

On the subject of new EU data protection legislation, which you raised with the Information Commissioner at the evidence session, I have previously written to the Committee on the forthcoming negotiations for a new instrument to replace the Data Protection Directive (95/46/EC). The UK Government has been consistent in emphasising the importance of evidence-based policy making, ensuring individuals' rights are protected, but stressing that the resource implications for organisations in the current economic climate must be proportionate to the benefits delivered by increased data protection safeguards. These messages were backed up by the Justice Secretary when he spoke to the British Chamber of Commerce in Brussels on 26 May and I enclose a copy of his speech.

We now expect the Commission to publish proposals for a new comprehensive legislative framework for data protection early in 2012. This will then provide the basis for negotiations between EU Member States and the European Commission, and will be subject to co-decision with the European Parliament. Although we do not have more detail on the likely contents of that proposal, the Ministry of Justice is preparing for the negotiations, informed by a Call for Evidence carried out last year on the current data protection legislative framework, which received responses from small businesses, large international organisations, local and central government departments, as well as members of the public and consumer groups. We have also discussed many of the issues likely to be raised with the ICO, which provided a very considered and useful response to our Call for Evidence.

We can expect the Commission's proposal to cover many of the issues the Committee discussed with Christopher Graham. I have already mentioned the investigative and enforcement powers available to the Information Commissioner. The question of how the Information Commissioner's data protection work should best be funded may arise in the context of a revision of the obligations on organisations to provide an annual notification to the data protection supervisory authority. Finally, the issue of fair processing notices, relevant to the question of whether insurers can pass the personal details of their customers on to third parties, may arise if the European Commission follows up the suggestion in its 4 November 2010 Communication that standard privacy notices be drawn up for use by

data controllers. The negotiations will no doubt range over these and many other topics, and I will of course keep the Committee updated as they progress.

As you discussed with the Information Commissioner, the Government announced earlier this month that it intended to ban referral fees in personal injury cases. With regard to the use of personal data in this context, the MoJ's Claims Management Regulation Unit and the ICO are members of a working group established to tackle unsolicited text messages and automated telephone calls marketing claims management and debt management services. The working group has representatives from other regulatory bodies and organisations, including the Office of Fair Trading, Ofcom and the Direct Marketing Association, and the telecommunications industry. At its recent meeting, the working group discussed how the members can work together to combat the problem, including using evidence gathered by mobile network operators. The group will meet again in a couple of months and, in the interim, a meeting between the regulators will take place to discuss consistency in regulatory approach and exchanging information. Separately, the MoJ and ICO are in the process of agreeing a memorandum of understanding to allow them, through sharing information and intelligence, to work together to tackle data misuse by authorised claims management companies.

Freedom of Information

I have written separately to the Committee on post-legislative scrutiny of the Freedom of Information Act 2000 (FOIA). As this work progresses, the Ministry of Justice looks forward to continuing to work with the Information Commissioner's staff and to receiving the Commissioner's considered view. Post-legislative scrutiny provides an excellent opportunity to assess how the Act has worked across the board, and may cover issues such as the offence of altering or destroying information in section 77 of FOIA, mentioned by the Information Commissioner in his evidence.

Independence of the Information Commissioner's Office

Finally, I have also written to the Committee recently on the revised Framework agreement between the ICO and the MoJ, which has now been signed off by both parties and is in force. I am confident that this, complemented by the relevant provisions in the Protection of Freedoms Bill, will see an enhanced independence for the Information Commissioner and his office in the future.

Rt Hon Lord McNally
Minister of State
Ministry of Justice

Formal Minutes

Tuesday 18 October 2011

Members present:

Rt Hon Sir Alan Beith, in the Chair

Mr Robert Buckland
Jeremy Corbyn
Chris Evans
Ben Gummer
Rt Hon Elfyn Llwyd

Claire Perry
Yasmin Qureshi
Elizabeth Truss
Karl Turner

Draft Report (*Referral fees and the theft of personal data: evidence from the Information Commissioner*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 24 read and agreed to.

Summary agreed to.

A Paper was appended to the Report.

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

Ordered, That the Chair 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 25 October at 10.15am.]

Witness

Tuesday 13 September 2011

Page

Christopher Graham, Information Commissioner

Ev 1

List of Reports from the Committee during the current Parliament

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

Session 2010–12

First Report	Revised Sentencing Guideline: Assault	HC 637
Second Report	Appointment of the Chair of the Judicial Appointments Commission	HC 770
Third Report	Government's proposed reform of legal aid	HC 681-I (Cm 8111)
Fourth Report	Appointment of the Prisons and Probation Ombudsman for England and Wales	HC 1022
Fifth Report	Appointment of HM Chief Inspector of Probation	HC 1021
Sixth Report	Operation of the Family Courts	HC 518-I (Cm 8189)
Seventh Report	Draft sentencing guidelines: drugs and burglary	HC 1211
Eighth Report	The role of the Probation Service	HC 519-I (Cm 8176)

Oral evidence

Taken before the Justice Committee

on Tuesday 13 September 2011

Members present:

Sir Alan Beith (Chair)

Jeremy Corbyn
Chris Evans

Yasmin Qureshi

Examination of Witness

Witness: **Christopher Graham**, Information Commissioner, gave evidence.

Chair: Welcome to the Information Commissioner, Chris Graham. We are very glad to have you with us again. We are very much depleted by Members serving on Bill Committees. There are several Bill Committees sitting this morning, which has had a drastic effect on our numbers.

Q1 Yasmin Qureshi: Good morning. I wanted to ask some questions regarding the practice of “blagging” that goes on. There has been a suggestion that some of the newspapers have been doing this or other bodies have been trying to get information illegally. Are you aware whether the police, the Press Complaints Commission or anybody has investigated any of the newspapers for blagging since 2006?

Christopher Graham: This is a section 55 offence. This is the unlawful accessing or disclosure of personal information without the authority of the data controller, to give it its technical term. We did a lot of work on that back in 2003–05 and in our publications *What Price Privacy?* and *What Price Privacy Now?* in 2006. To answer your question about press behaviour, apart from repeating the call that we made in 2006 for an effective deterrent to this in the form of the potential for a custodial penalty, at various stages, in two public consultations launched by the Ministry of Justice, we have repeated that point.

So far as the Information Commissioner is concerned, the activities of the press have not particularly come to our attention. My great concern about section 55 which remains is not really very much to do with the press. There is lots and lots of evidence of section 55 being breached on quite a routine basis, but it is really about financial services, debt collection, claims management companies, and also some quite worrying interference with the course of justice, perhaps attempted jury nobbling or witness tampering. That is the real issue.

I would like to draw the Committee’s attention to a case that came up yesterday before the Brighton magistrates of a section 55 prosecution, because it is pretty typical of what is really going on. I am not suggesting that the concerns about press standards are not real, but it does not really involve the Information Commissioner’s Office or blagging these days. It is much more a question of hacking, which is being investigated in another part of the wood. Yesterday’s court case in Brighton involved an employee of a high street bank whose husband had been jailed for a

sexual assault. The 18-month prison sentence was being appealed by the victim as being unduly lenient, and subsequently the sentence was increased from 18 months to two years. While that appeal was in train, it appears that the bank employee was quite routinely accessing the accounts of the victim, who was a customer of her branch of the bank in Haywards Heath. It is being reported in the press today.

When that came to our attention, and we investigated and we prosecuted, under the Data Protection Act as it now stands, of course, a fine is the only available sentence. I am very disappointed that the going rate for a section 55 offence in the magistrates court has just gone down from £150 to £100. This is simply no deterrent. The case yesterday involved eight counts of a breach of section 55, £100 a count. Two months ago in July, in Bury, the former partner of an NHS walk-in centre worker was prosecuted under section 55 and the going rate then was £150 per count.

This simply is not a deterrent. The problem that we have is that the courts are bound by the fines laid down in the Act and they have to take into account people’s ability to pay. There is nothing but the fine; that is it. You cannot then access the full range of potential community sentences, tagging, curfews or whatever, because Parliament has not commenced sections 77 and 78 of the 2008 Criminal Justice and Immigration Act. By ministerial order, subject to the negative procedure, that could be accessed in pretty short order.

I am very concerned that this is now getting caught up in the reeds of the Leveson inquiry. This sort of thing does not have anything to do with the press. I know it was all stopped back in 2008 because the press were concerned that there was going to be a chilling effect on their ability to investigate matters in the public interest, but sections 77 and 78 provided a way forward. I am now concerned that everything stops because of Lord Justice Leveson’s inquiry and we cannot get on with putting in place this very necessary deterrent. It just beggars belief that, when more and more organisations have a right to our personal information, to access and process it, the courts do not have the full range of potential sentences to deal with an offence which can involve any of us. This is not about celebrities’ hospital appointments. This has the potential to wreck people’s lives. The basis of the appeal in the court yesterday was that the victim was saying her life had been destroyed. The

suggestion is that the attacker's wife was breaching section 55 of the Data Protection Act to see whether the victim's allegation that her life had been ruined was supported by the facts of her patterns of expenditure. Parliament cannot just sit back and watch this sort of thing happen. You cannot subcontract that to a High Court judge. Sections 77 and 78 of the 2008 Criminal Justice and Immigration Act are there to be commenced, and it is in your power to do that.

Chair: It is in Parliament's power to do that.

Q2 Yasmin Qureshi: In light of the concern that you expressed about the prevalence of blagging across different groups such as debt collectors, solicitors, insurance companies—clearly you are very concerned about what needs to be done—you would be pressing for that particular provision to be fully implemented. Are you planning to do another report into this illegal trade in information?

Christopher Graham: I don't think it's a question of another report. We have already heard the Prime Minister, the Deputy Prime Minister, the Leader of the Opposition and the Home Secretary regret that they did not take any notice of the 2006 reports. Subsequent to that, we have had two consultations from the Ministry of Justice and we have put in our submission. This is now my third appearance before a Select Committee making the case for the commencement of the custodial penalty.

The Information Commissioner has said enough on this issue now. The ball really is in the court of the Ministry of Justice and Parliament to decide what they do about the evidence that we have presented.

Q3 Chris Evans: You have gone into some detail, saying it is a major trade in illegal blagging. Do you think in some ways we are behind the times, as when an illegal trade develops it becomes very sophisticated very quickly and calls for sophisticated and complex solutions rather than simple solutions? Do you think in some ways the Government have already missed the boat on this?

Christopher Graham: The Government, to be fair to them, have been doing quite a lot in different areas to reflect the fact that we are all doing our business online. We are all interacting with the public authorities and with private companies. Everything we do really is online. What the Government have been doing in response to the points that the Information Commissioner has made about rogue employees, carelessness and so on has been to explore the possibility of the restitution of the proceeds of crime, under the Proceeds of Crime Act. We have had one case, the T Mobile case, prosecuted in Chester Crown court in July, where we got a significant payback from rogue employees in the telecoms area. They are also investigating making section 55 offences recordable offences, which would be good. I believe the Secretary of State has approached the Sentencing Council. I am not saying the Government have not done anything. I am just saying that the courts are inevitably going to impose very minimal sentences where they naturally have to take into account people's ability to pay if they do not have access to the full range of alternative sentences, because the Act

currently says there can be a fine of up to £5,000 in the magistrates court, higher in the Crown court, but the courts are not encouraged to take these offences very seriously, whereas, of course, they can completely ruin people's lives.

If you look at the Haywards Heath case, there was a woman who had been put through hell by her attacker, and she has to go through a different sort of hell because the bank that she trusts is able to access all her very private stuff and work out her patterns of expenditure and what she is doing with her time as well as her money.

Q4 Chris Evans: Do you offer any training to any companies where you feel that blagging is prevalent? Do you think it is possible to profile a rogue employee, as you say?

Christopher Graham: We produced a DVD back in 2006, *Blaggers Beware*, and we are updating that at the moment. Companies spend an awful lot of money on data protection. They can then be let down by individual carelessness or by rogue employees. I do not say you can guarantee to be able to spot a rogue employee. Presumably if you could, you would not hire him or her in the first place. Possibly, in addition to induction and training, you do need to have very regular checks, perhaps mystery shopping with databases to see who is accessing them and why. It should be very clearly part of the ongoing process of people management in organisations.

Sometimes people regard data protection as a rather arcane matter or else just a piece of bureaucracy, and so long as you tick the boxes and go through the motions that is fine. But there are very real victims when things go wrong. That is why the Information Commissioner's Office takes this very seriously, whether it is imposing civil monetary penalties on data controllers who get things wrong or whether it is prosecuting vigorously where individuals have been abusing their position to access information which they should not be doing.

Q5 Chris Evans: If you take an example, I started my career in a bank and it probably was a more powerful position in terms of having access to personal data than I have now as a Member of Parliament. In my office at the moment I employ four members of staff. I can keep an eye on most of them in terms of the data they are processing, but how do you tailor solutions for an industry like the banking industry, with thousands of employees? Do you think there should be different solutions for different industries, or do you think there is a "one size fits all" answer to this problem?

Christopher Graham: All data controllers have to be aware of the risks. I know you all notify with the Information Commissioner's Office. You run small offices and it is very important that you and your colleagues take these data protection issues very seriously. You are, through case work, dealing with very sensitive, personal information.

We can be helpful. The Information Commissioner's Office makes all sorts of resources available to help people to keep information safe. We now have a programme of very professional audits of data

13 September 2011 Christopher Graham

controllers, large and small. It is a free service. It is the only free consultancy you will get. We are urging the big financial services companies to allow us in to audit their compliance with the Data Protection Act. Where there are problems we can then identify those, as any auditor would. There is a work programme. It then should be a badge of pride: “We have been checked over by the Information Commissioner’s Office”, which then gives confidence to customers. It is a win-win all round.

The Information Commissioner’s Office is not just looking around for people to prosecute. We are here to help. We want to educate, empower, enable and engage as well as enforce.

Q6 Chair: Can I turn to Europe? The Committee in the past has looked at European developments in data protection. We are now faced with the possibility of a European directive. What is your view about developments in this direction, and what do you think the British Government should do?

Christopher Graham: The Commission will be publishing its proposal probably in November or December. Then the fun begins with the negotiation over the framework directive which will set the course of data protection law in the period to come, although it will take a number of years to negotiate. We are very much engaged with that process. We are members of the Article 29 Working Party which advises the Commission. We hope very much that the proposal that emerges will be clear about the principles and reasonably future-proof. We do not want something that is so specific that it is immediately out of date because technology and business practices are changing so fast.

It would be appropriate in the spring, when we see what the proposal is, for the Information Commissioner’s Office to hold some sort of conference to bring the various stakeholders together so that we can be clear about the way that things ought to go and we can no doubt advise Government in the negotiations. It clearly is the big event for the back end of this year and the beginning of next.

Q7 Chair: Is it likely to land us with procedures that merely complicate without improving our own regime?

Christopher Graham: I hope, in the best principles of the seven habits of highly effective people, they will begin with the end in mind rather than be very specific about the means. The technology and what you can do online are changing so fast that the current rules are very much out of date. If the new directive or the regulation, or whatever it is, is overly specific as to particular procedures and not clear enough as to principles, then we will be in that outdated position again very quickly.

The important thing is to establish some principles—for example, the accountability of the data controller—and to make it the responsibility of the data controller to ensure that they are conducting their business in accordance with the principles under the Data Protection Act, rather than say to data protection authorities, “It is your job to sign off on everything and tick every box before things happen.” The

developments we are seeing in globalisation, cross-border transactions, processing in the cloud, as they say, mean that the old-fashioned, prescriptive way is clearly not the way of the future. The role of a data protection authority like mine in the regime that we advocate will be to keep data controllers up to the mark on a risk-based basis, rather than say, “We do what we do. You cannot do that there. We have to sign off on that and we will tick this box.” That is clearly not going to be effective, whereas being very clear about the principles and the responsibility of data controllers and having effective data protection authorities properly funded, who can hold data controllers to account, is what we are looking for.

Q8 Chair: You mention the international nature of much business now. Does that leave an open back door in the absence of a new directive through which incursions can be made into data which would be illegal if carried out in the UK, but which can be achieved because of less stringent regimes in some other countries?

Christopher Graham: There is a lot of international co-operation and a lot of work done by the Article 29 Working Party in establishing the adequacy of different data protection regimes worldwide. The issue very often is not the adequacy of a national regime; it is the adequacy of the arrangements made by a particular data controller. It is not acceptable for a data controller to say, “It was okay leaving me and I didn’t know very much about the data processor I was dealing with or where the work was being carried out.” The data controller should be held responsible for what happens to data that they have collected and are using.

I am going off to meetings tomorrow in Europe. We have to co-ordinate across the 27 member states of the European Union, but also it is very important to have good international contacts outside Europe. There is an upcoming international conference in Mexico City where I am leading a session. We are not little Englanders in this. We realise we are dealing with a global business and we need to make sure the messages get across worldwide.

Q9 Jeremy Corbyn: Only a fifth of private companies contacted by your office apparently took up any offer of a free audit and advice; yet the response from public sector organisations to your offers is apparently much better. Do you have any concerns about the level of private sector protection of data?

Christopher Graham: I very much regret that they are so backward in coming forward. The public sector has responded better. Some of them have to. Whitehall Departments don’t have a choice. I don’t have a general power to inspect without it being a consensual audit. I am concerned that some of the problems that are taking place, yes, are in the public sector—local government is particularly bad—but the private sector, too, is not as good as it thinks it is. The Barclays Bank case yesterday should give high street banks some pause for thought.

I simply cannot understand why you would not accept a free audit from the Information Commissioner. If I

find something horrible, I am not going to impose a civil monetary penalty there and then. We are going to agree a work programme for you to get it right. It is very short-sighted of private companies not to engage more with the Information Commissioner, because their customers are engaging with these issues. Their customers will fall out of love with even familiar high street brands that do not respect them enough to take privacy seriously.

Q10 Jeremy Corbyn: Where a private company has a significant public sector contract—and many do; they are perhaps operating in local government services, parts of the health service, that sort of thing—do you have any particular locus for putting slightly more encouragement on them to co-operate with you in those respects?

Christopher Graham: In a private company undertaking a contract for a public authority, the responsibility for the security of citizens' information would remain with the data controller. We have had to issue a civil monetary penalty on two London local authorities. I know it's the public sector, but it makes the point. In Ealing and Hounslow, one council had contracted with another to deliver a common service. Just because council A fouls up does not mean that council B is not responsible if council A was processing council B's information. There are issues on where responsibility lies.

The point you make is also very relevant in the freedom of information area where public authorities, particularly under the Big Society umbrella, are dealing with any willing provider, private contractors, charities, third sector organisations and whatever. We have to be very clear that that does not exempt the public authority from its obligations under the Freedom of Information Act. You cannot subcontract your responsibility either for data protection or for freedom of information.

Q11 Jeremy Corbyn: Going back to the private sector issues for a second, if there is only a fifth take-up in the private sector, I realise that you have powers of encouragement. Is there any more you can do, such as badging, certificates, that sort of thing? It seems to me a whole area of public concern that private companies are not taking up your offers and therefore their data is potentially at risk.

Christopher Graham: The penny is beginning to drop with big companies that the public are very alert and concerned in these issues, and if they don't catch up with the public they are going to lose business. That usually is the sort of language that they understand. The Information Commissioner's Office has always taken the view that there ought to be the power of inspection. If we think there is a problem, I should not need to get a warrant to break the door down. The Information Commissioner, as the data protection authority, should have the right to come in and check on compliance.

It may well be that under the new directive that power will be given. It is power that we have in some areas, and sometimes we can negotiate ourselves in. That is what happened with Google. I did not have the right to audit Google Inc, but Google got themselves in such a

difficult position that in the end they could not say no. There are ways and ways of doing it. It would be preferable, and I hope that under the next data protection regime we will get it, that the Information Commissioner's Office would have the power to inspect whether or not invited.

Q12 Jeremy Corbyn: You mention public sector local authorities, but when it comes to health authorities it seems to me that there is endless scope for wrong releasing of information, because they send out endless text messages, e-mails, faxes, reminders for appointments and things like that. I can understand why they do it, but often that highly personal information can quite easily get into the wrong hands as a result. Do you have concerns? Do you give any general advice to the NHS in this respect?

Christopher Graham: I do, and I am very worried about the NHS. I raised the issue with the chief executive of the NHS, Sir David Nicholson, who was very responsive to my concerns. We have written a joint letter to all managers in the health service saying that this is really important. It is particularly important at the moment at a time of change and reorganisation. We had the shocking example of a hospital in Belfast, a cancer centre, where the local health authority was withdrawing from the hospital but they forgot to remove all the patient files of cancer patients. This is the Belvoir Park hospital in Belfast. They withdrew from the hospital and abandoned it. When the local vandals got in and started stripping out anything of value, they found all the patient notes for all the cancer patients. It is a huge issue. Presumably the data was not very high up on anyone's risk register. When they left the hospital they thought they had abandoned their responsibility for those files, but in the health service all the time we are hearing of patient notes being left in a skip.

We had a case in Manchester of a medical student who was working for South Manchester NHS Teaching Trust. He lost a whole load of patient data on a memory stick and it was unencrypted. The answer was that the hospital thought the university would have trained the student in data protection and the university thought the hospital would have done. Because the health service is so big and naturally dealing with sensitive personal information all the time, it is a really important issue.

Q13 Jeremy Corbyn: You offer training to both hospitals and GP practices. It seems to me that GP practices are very vulnerable in this respect. They have often a very large turnover, particularly of reception staff, and there is a huge area there of potential for wrong release of personal information.

Christopher Graham: Yes, and pharmacies too, because it is just sort of chatting. To get back to the journalism issue, it was well established that one of the easiest ways of getting a story is just to ring up the GP practice or the hospital and say in a sufficiently confident voice, "It's about those tests," and you will be given the information over the phone. You ask whether we are able to train. Yes, we are there to educate just as we are to enforce. If we can solve the problems before they arise, that has to be a more

13 September 2011 Christopher Graham

sensible approach. It is very much stick and carrot. Yes, there is a £500,000 civil monetary penalty there when things go spectacularly wrong, but I would much prefer to help everybody to understand the importance of these issues and to see that playing fast and loose with people's personal information is not a victimless crime. These are real people, with real personal issues which they would prefer to keep private, thank you very much.

Q14 Jeremy Corbyn: Would you favour a power or an encouragement for, say, local authorities where they are contracting out a service or part of a service or buying a service in from the private sector that they would be able to put a requirement in the contract that they had to co-operate with yourselves on information storage systems, training and all that sort of thing as a way of upping the threshold of protection of personal data?

Christopher Graham: It would be very good to have data protection on a procurement list of things to think about, but the contracting authority has responsibility as a data controller and so does the contracting company. One of our first civil monetary penalties was applied to the private company, A4e, who were very much involved in getting people back to work, providing services to quite disadvantaged people and, glory be, a laptop goes missing. It is both the contractor and the contracting party who have obligations under the Data Protection Act. I am not a great believer in getting people to sign up to a statement, "Yes, I understand I am subject to the Data Protection Act." You just are subject to the Data Protection Act. I can certainly help in raising awareness and providing training. Our website is a very good resource for information here. I would like to get these issues raised higher up the list of concerns that people have in these difficult times. It is not a nice add-on, it is pretty fundamental, both to private businesses and also to public authorities, to get this sort of thing right. If they don't, they are in trouble with the Information Commissioner, but they are also in trouble with their customers and their constituents.

Q15 Chair: Can I clarify on general practice? In the NHS, general practices are subject to data protection, but are they not subject to freedom of information in respect of their private business, which is what they are?

Christopher Graham: Freedom of information covers public authorities. I would need to check back to see whether individual GP practices are public authorities. I suspect they are not.¹

Q16 Chair: I don't think they are. For that reason, as far as I can recall, FOI does not generally apply to them, whereas data protection does.

Christopher Graham: No, but subject access does under the Data Protection Act, so you will be entitled

to say, "I need to know what you have in my files." You are certainly entitled to expect that the seventh data protection principle will be observed. That is the one around security of information. To be fair, doctors are increasingly aware of their responsibilities. You have the system of Caldicott guardians. When I first came in as Information Commissioner and registered with a GP practice in central Manchester, the GP when he heard what I did very proudly said, "You will be glad to know I am a Caldicott guardian." I did not know what a Caldicott guardian was at the time, but I do now. Doctors in the health service do take this very seriously, but the health service is not just doctors, it is also a lot of support workers, receptionists, practice nurses and so on. There is a big job to do there.

Q17 Chris Evans: The MoJ is currently preparing a memorandum on post-legislative scrutiny of the Freedom of Information Act. Have you been involved in this and what conclusions do you think or hope it will draw?

Christopher Graham: I am aware that the Ministry of Justice is drawing up a memorandum which may come your way or may come the way of a Joint Committee of both Houses for post-legislative scrutiny. I have not been involved in the process. I am very keen to contribute to the process, because it is good after 10 years or so to see how the Freedom of Information Act is going, and there are all sorts of ideas for improvement. I am sure that, however that work is taken forward, it will be very important and we would like to be involved in it.

Q18 Chris Evans: Even though you are at the coal face, you have not been involved in any way in post-legislative scrutiny of the Freedom of Information Act. I find that a bit strange. You are dealing with it day to day and yet you have not been involved.

Christopher Graham: I would expect to be giving evidence to this Committee or to another Committee. What is happening at the moment is that the parameters of the debate are being scoped by the Ministry, and I don't think I would expect to be involved in that specific process, but the Ministry is very well aware of where there are the stresses and strains. I am quite relaxed about this because I will not be backward in coming forward in terms of saying what I think when we get into the process of post-legislative scrutiny.

Q19 Chris Evans: It has been a much maligned Act. Some people love it; some people hate it. It is like Marmite, I suppose. You said "stresses and strains". Could you cover some of the main areas where you think there have been stresses and strains and what you think particularly has been wrong and right with the Act, in general themes?

Christopher Graham: The major problem that we faced in the Information Commissioner's Office was that we were far busier than we expected we would be because the whole public service made much heavier weather of dealing with freedom of information requests than anyone anticipated. When I came before this Committee two and a half years ago, the whole system was grinding to a halt. I undertook that what I

¹ *Note from the witness:* GP practices are covered under FOIA—Schedule 1 Part III, FOIA para 44. We also highlighted the importance of new GP consortia being subject to the Act in our recent response: www.ico.gov.uk/about_us/consultations/consultation_responses.aspx to the DOH consultation: 'Transparency in outcomes—a framework for the NHS'

was going to prioritise was sorting out, managerially, the great backlog of freedom of information requests. I think I can claim that, working with my staff in the ICO, we have very largely achieved that over two years. There are still some cases that come to the Information Commissioner's Office and it all takes too long, but, whereas it used to take years, we now have no cases that are older than 12 months. We are tackling those cases that are taking nine months, eight months and so on and driving down the backlog at a time when there is an increasing number of cases that come to the Information Commissioner's Office on appeal from the decision of public authorities.

The business in the second quarter of the calendar year was about 10% up on the previous 12 months. It is a growth business. One of the stresses and strains is getting through the business. We have done it by simplifying our processes. We have also been much stricter with public authorities and we are insisting on timely responses. We are not afraid to tell truth to power when we are dealing with some very big beasts indeed—for example, the Cabinet Office. So the whole process has speeded up.

Where there are stresses and strains, apart from just the amount of business, is that, in the middle of a recession, many public authorities think they have better things to spend their money on than freedom of information. That is a bit misguided, because transparency and accountability are aids to efficiency, but you have to accept that it is not just a back office activity; it is pretty key to make sure that you put appropriate resources there. I do understand I am dealing with some very stressed public authorities who are finding it very difficult to keep up.

Post-legislative scrutiny will want to look at some ways in which the regime operates. Let us see how that goes.

Q20 Chris Evans: You have seen a 17% increase in complaints. Do you think that is down to people knowing their rights, or do you think it is companies and local authorities failing to comply? What do you think the reasons are behind that?

Christopher Graham: It is a bit of both. Public authorities could save themselves an awful lot of trouble if they spent less time thinking of excuses for not making information available and pro-actively published much more than they do. Very often it is the hunt for what you believe you are not supposed to know that is so fascinating, whether you are a journalist on a local newspaper or whether you are a concerned citizen. It is exciting to make the authorities reveal things they would prefer not to reveal. The information is probably deeply boring, and if it was revealed anyway, it would save an awful lot of time.

It is undoubtedly the case that citizens are waking up to their powers under the Data Protection Act to demand access to their own files, and under the Freedom of Information Act to inquire about decision-making processes. I suspect that what went on in this place a few years back rather whetted the appetite of citizens who realised that they did have rights under the Freedom of Information Act and they could find out things that their lords and masters would perhaps

prefer they did not know. What happened here probably contributed to the process.

Q21 Chris Evans: If you had a wish list, what one change would you make to any Act or regulation which would impact positively on the work that you do? Is there anything particularly that you can think of?

Christopher Graham: If you are talking about data protection as well as freedom of information, I have said I would like to see sections 77 and 78 of the 2008 Criminal Justice and Immigration Act commenced. That is at the top of my wish list at the moment. A change which I would like to see on the freedom of information side is attention given to section 77 of the Act, which deals with the unlawful destruction and obstruction of the release of information under the Act, which I cannot do anything about if the offence took place more than six months ago.

It is a slightly arcane point, but if there had been misbehaviour in a public authority and information that had been requested was then conveniently lost or destroyed, that is a section 77 offence. I have to get there within six months or I cannot prosecute. It is very difficult to do that, because it probably doesn't come to me to be investigated until it has gone through the request of the public authority and the internal review. Then it comes to me. If we think there has been some misbehaviour, it may have passed the six-month deadline. Instead of being an offence that is prosecuted in the magistrates court, it ought to be an offence that is prosecutable either way in the magistrates court or the Crown court, so that factor did not have to be taken into account. I am sorry, this is real geeky stuff, but that would make a considerable difference, because everybody would know then that, if you were stupid enough to delete data which had been requested under the Freedom of Information Act, the Mountie was going to get his man.

Q22 Chair: Can I turn now to something which the House will be considering later today? The Government has already indicated that it is prepared to ban referral fees by insurance companies, but that raises the question, which you refer to on your website, whether some of the people who are passing on personal information about those who have had accidents might be acting illegally when doing so. That could apply to insurance companies, garages, car hire companies and towing companies. These all appear to be sources of information, usually paid for by the claims management companies who collect the information. Whereas it may be desirable to ban the fees which are paid for this, if the whole process is illegal, that puts it into even sharper focus.

Christopher Graham: It is illegal, but it is highly profitable. Until the referral fees are abolished, it is obviously hugely profitable. There is not much of a deterrent. If you are working for a car hire company, a towing company or a repair garage and you think you could get in and make that claim for the referral fee, it is a high-profit, low-risk business. That was what was going on with the NHS walk-in centre in Bury. We were investigating the nurse who was passing on information to her boyfriend, who was

13 September 2011 Christopher Graham

selling the information to a local claims management company. The prospect of getting a £150 charge per count in a magistrates court is not much of a deterrent when you are making hundreds and hundreds of pounds on these referrals.

That is a very good example of what the section 55 issue is about. It is not about celebrities and their hospital appointments. It is about citizens' car insurance premiums. That is why I simply cannot understand why it is so difficult to commence those proposals under the 2008 Act. I am sorry it is becoming a bit of a gramophone record, but it is so easy to do and it is so obvious. It is for the benefit of the citizenry. The insurance issue is complicated because part of it may be that, deep in the small print of what we sign up to within an insurance policy, there is, "The company reserves the right to assist you in a claim by providing your information to a lawyer." I cannot say I read very carefully to page 14 of an insurance policy to see whether that is the case. The insurance companies will say, "We have the consent of the insured driver," but we are dealing with two other things that give me concern. First of all, it is all the other parties who are getting in first to claim the fee. That is clearly going on, but it is very difficult to pin down. Until you have an effective sanction for section 55 offences, there is not an awful lot more I can do about it. Secondly, there is the question of spam texts. A lot of the concern has been driven by these texts that appear saying, "Our records show that you are in line for a compensation payment of £4,750 for that accident you had. Text CLAIM or STOP." If you text either, you are confirming that you are there and providing a marketing lead, because these are randomly generated texts. People who have had a car accident think, "Good heavens, how did they get that information?—That is disgraceful", but it is probably just that random text.

We are working very hard with Ofcom and the telecom companies to try to get to the source of these spam texts, but it is a bit like looking for the launch sites of V2 flying bombers in the second world war: we will get there, but it is taking us a long time.

Q23 Chair: You mention insurance companies including provisions in contracts, with or without box ticking—it could be either way—which give them the ability to pass on information. Is that not something you should work with the insurance companies on?

Christopher Graham: We have contacted the Association of British Insurers following MP Jack Straw's intervention on the issue, because he talked about insurance companies having admitted to the insurance industry's dirty little secret. We are trying to find out from the Association of British Insurers what they have to say about that, and frankly they are not being very helpful at the moment. I don't know whether the Government announcement about referral fees will change their tune.

This is where I am frustrated that I do not have the power to inspect. We have invited a number of insurance companies to undergo voluntary auditing and, surprise, surprise, they are not interested. There is sufficient concern now in Parliament for this issue

to be brought to a head. I expect to get greater co-operation from reputable brands in the insurance business.

Q24 Chair: They are arguing that they would like to get rid of referral fees, but they may have hidden in their contracts provisions absolving them of any legal responsibility for giving away the information in the first place.

Christopher Graham: Potentially it is a breach of the first data protection principle. It is not fair processing if you claim consent and all your policy holders say, "I don't know what you're talking about—I never knew." Frankly, I am fed up with hearing from the car insurance companies, "We just can't help ourselves—it's the system, you understand." The Information Commissioner will help you get off this drug, but you need to co-operate with the ICO.

Q25 Chair: I still find it quite striking that we are in a situation where we are looking to remove the fees for a practice which may itself be illegal.

Christopher Graham: I suppose it could be argued that the fees are aiding access to justice. That is really outside my territory. You could have a system of perfectly legal fees but nevertheless that encouragement breaches section 55 of the Data Protection Act, which is certainly an offence. Both could be true. The Government says it is going to abolish referral fees. I would also like it to take section 55 offences a little more seriously than it is taking them at the moment.

Q26 Chair: You outlined some concerns about the Protection of Freedoms Bill in evidence to the Public Bill Committee. Do you think you are making any progress on that?

Christopher Graham: I am not sure. The Bill seems to be taking an awfully long time. It is coming back for report stage in the Commons next month. Then it goes off to the House of Lords. We are a bit disappointed that we are not seeing progress on issues that we are concerned about. Very often the devil is in the detail but I do emphasise the devilishness of it. I applaud the intentions behind the Bill, but some of the intentions appear to be frustrated by either the lack of detail or specific reservations that stop the solution being as good as it could be. We have concerns over the DNA regime where it relates to innocent people or people who are no longer of interest to the police, where it is proving very difficult to get a solution that ensures that the record on the police national computer also gets deleted. I have concerns around CCTV and automatic number plate recognition, where the consistency and comprehensiveness of the approach are concerns. I don't see how it runs alongside the Information Commissioner's code for CCTV. It is a regime that will apply not to every sector, England and Wales only, and so on. I am concerned that the proposals on criminal records disclosure don't really seem to be taking into account the recommendations of the expert adviser who produced the report *A Balanced Approach*. The approach seems to be anything but balanced.

I am still hoping that we will get a better solution for filtering out old and minor convictions from employer vetting checks. It is absolutely vital that we get progress on what we call enforced subject access. For example, if the law says the employer cannot check out your past but he can say, "If you want this job, you exercise your rights under the Data Protection Act and bring the results to me," that ought to be banned. I am holding my breath on the proposals for the enhanced independence of the Information Commissioner, which is very much at the back of the Bill, and I hope it is still there at the end when it becomes an Act.

Q27 Chair: This Committee is on record in the past as having argued that the Commissioner should be a creature of Parliament, like the Ombudsman, rather than answerable to a Department.

Christopher Graham: A creature of?

Chair: In the sense of being created by and owing its independence to Parliament.

Christopher Graham: We are making some progress on the general point. Reference is made to a framework agreement. We have reached agreement with the Ministry of Justice on a framework agreement. That will be in the Library of both Houses before too long. It does give me greater confidence about relations with the Ministry of Justice, but the Ministry of Justice, frankly, is not my problem. My problem, if it is a problem, is, if I am not seen as an officer of Parliament, reporting directly to Parliament, I have to negotiate my way through with many other Departments of State. I have to deal with the Cabinet Office Efficiency and Reform Group controls on marketing activity, which apparently cover the Commissioner's responsibility to offer advice and guidance. I have to get a tick on anything I propose to do.

I am concerned about my website being dragged into some monster Government website, alpha.gov.uk. I am sometimes concerned about aspects of the transparency and accountability drive, where I applaud the direction of travel, but I find sometimes a confusion between the right to know and the right to privacy. The Information Commissioner has a bit of work to do to help clarify where the citizens' rights are there.

Q28 Jeremy Corbyn: Are you asked to make recommendations on that distinction?

Christopher Graham: I am going to make recommendations on that distinction.

Q29 Jeremy Corbyn: To whom?

Christopher Graham: There is a consultation at the moment launched by the Cabinet Office about the approach to transparency and open data. We will certainly be making our views clear on that. There are some general points here. There is a lot of good work being done under the banner of transparency, accountability and open data, but sometimes the

enthusiasm of the modernisers rather brushes aside the issues around privacy.

For various Departments of State to say very wisely, "There is a balance to be struck between the right to know and the right to privacy," does not say where the balance should be drawn. That is what the Information Commissioner is there to do, and that is what I certainly will do.

Another point I should make before I finish is that we all have to operate in very difficult financial circumstances. All public authorities have to do better for less and that is what we are getting on and doing. I have to make a saving of £250,000 on the freedom of information side of my budget which is paid for by grant in aid by the Ministry of Justice. From my current budget, which is £4.5 million, it is a pretty significant cut following a cut this year and there are more cuts to come.

We are certainly getting on with making changes so that we can achieve value for money, but I would make two points, if I may. I have highlighted in the foreword to this year's annual report the unsatisfactory nature of the hybrid funding that funds the ICO with three quarters of the money coming from notification fees for data protection and a quarter coming from grant in aid for freedom of information. Under public spending rules I cannot treat information rights as the seamless project that it is. I have to work out that this bit is data protection and that bit is freedom of information. Sometimes that has a perverse effect. In order to save a pound of freedom of information money, I probably have to save three pounds of data protection money just when everyone is screaming at me to help to publicise and give guidance on data protection.

It is time to look at the way we fund the ICO. Possibly the new directive will give us a way forward on this, but I am spending far too much of my time trying to work out apportionment of costs between FOI and DPA in order to keep the National Audit Office happy. I am not rattling the tin. When I came before you two years ago, I remember I was put under a lot of pressure to say, "Don't accept this job until you have a guarantee on the funding." I said, "No, there is a management issue here. I will sort that out first." I am still not rattling the tin, even though we have sorted out the management issue and we have this big increase in freedom of information business, but I will make the business case for additional resources if I am asked to take on additional responsibilities, either as a result of the post-legislative scrutiny under FOI or as a result of transparency, accountability and open data. I will look after the efficiencies and the growth in volume, but what I cannot look after from my own resources is the additional responsibilities that look like they are coming my way. I will make business cases to say that I will take on those responsibilities but I need the budget to do it.

Chair: Mr Graham, thank you very much indeed for your helpful evidence this morning.

ISBN 978-0-215-56197-8



9 780215 561978

