



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Freedom of Information and Privacy – the Regulatory Role of the Information Commissioner

Richard Thomas
Information Commissioner

Centre for Regulated Industries

9 January 2008

It is a real privilege to be asked to address such a distinguished audience from the world of regulation. I have been asked to speak on the subject of Freedom of Information and Privacy – the Regulatory Role of the Information Commissioner. This is a very broad canvas, which inevitably includes both description and analysis.

Law and status

I will start with a reference to the relevant law which sets out my responsibilities and the status of the Commissioner. There are four principal legislative instruments – the Data Protection Act 1998, the Privacy and Electronic Communications Regulations 2003, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. Information flows are ever-more global and three of these measures largely implement European Union legislation. Only the Freedom of Information Act is home-grown UK law, but that also has a strong international flavour - largely reflecting corresponding laws in other parts of the English-speaking world. The Data Protection Act 1984 originally created the post of Data Protection

Registrar with a narrower remit. The title was subsequently changed to Data Protection Commissioner and, with the Freedom of Information Act, the title changed again to the Information Commissioner. The post is perhaps somewhat anachronistic in some respects as a sole Commissioner. Most of the former Directors General in other areas of regulation were converted to Boards or Commissions some years ago. I would not wish to call myself a dinosaur – indeed there are others who are sole practitioners like myself, such as the Parliamentary Ombudsman - but I do recognise that we are perhaps an unusual species these days.

The independent status of the Commissioner is very important and taken seriously. It is a requirement of the European Directive on Data Protection that there should be an “independent supervisory authority”. Independence is equally essential to make Freedom of Information meaningful where it would be neither feasible, nor credible, for the Commissioner to be a civil servant or otherwise part of government. Independence is therefore achieved through appointment by HM Queen, direct accountability to Parliament and quasi-judicial tenure. The Commissioner is appointed for a fixed term and can only be removed from office by Her Majesty in pursuance of an Address from both Houses of Parliament.

The Information Commissioner directly employs staff, though job numbers and salary levels are controlled by government. The Information Commissioner’s Office - the ICO - now has about 270 staff. Most of my staff are based in Wilmslow (just outside Manchester) where the office started in 1985. We now also have regional offices in Edinburgh, in Belfast, in Cardiff and a small outpost at Millbank Tower in London. My office has two separate revenue streams. Data protection is funded by a £35.00 flat

paid by data controllers each year when they notify their processing of personal data. Freedom of information is funded by annual government grant-in-aid.

Functions

The 'Governance of Privacy' by Colin Bennett and Charles Raab examines the different types of role for Privacy and Data Protection Commissioners. These can be broken down into three main headings which are a good summary of the legislative functions which we are required to administer for both Data Protection and Freedom of Information. The first broad heading is **Promoting Good Practice**. Both the main Acts explicitly spell out a statutory duty responsibility to promote the following of good practice. This is widely defined in terms of compliance with the law and such practice as appears to the Commissioner to be desirable. This duty, with more specific provisions, embraces the educational role relating to both individuals and organisations. It also embraces other roles identified by Bennett and Raab, such as policy adviser, legislator (issuing and approving codes of practice) and a certain amount of negotiation. Secondly, there is an **Ombudsman** role - the adjudication of complaints. Thirdly there is a direct **Regulatory** role – which includes securing compliance, acting as auditor taking enforcement activity and sometimes acting as prosecutor for criminal offences in both Acts.

Taking the broader title of "Regulator" this is quite an unusual hybrid of different sorts of function. We are keen to see ourselves as a "Strategic Regulator". We have re-structured to reflect the different types of function, with dedicated staff in each of those areas and across both main disciplines. As part of our strategic approach, we are now more selective towards data protection complaint-handling, recognising that

(although we receive over 25,000 cases a year) we cannot award compensation and our powers to award any other form of redress are very limited. This also reflects that other functions can create more of an impact in terms of systemic improvement than the resolution of individual cases. So much more of our resource now goes into the promotion of good practice and, where necessary, the regulatory role where we need to either threaten or take formal enforcement action.

For freedom of information we do have stronger powers of adjudication and the main focus is currently on the resolution of complaints. But here also this will gradually shift more into more of a promotional and enforcement role.

Tensions and common ground

Can the same Commissioner cover both freedom of information and data protection at the same time? Is there not a conflict between the two subject areas – with one focused on openness and transparency and other on privacy and confidentiality?

Let me start by saying that there is in fact quite a great deal of common ground.

Both involve the growing discipline of information rights – or rather the information duties and obligations on those who are holding either personal or official information. Both are heavily concerned with transparency and access. Both have a wide horizontal impact affecting virtually every aspect of public, commercial and private life. We deal with some 115,000 different public authorities under freedom of information. This covers not just central government and every part of local government down to parish councils, but also the entire world of public education, every part of the National Health Service down to doctors' and dentists' surgeries, every police force and police authority, every non-departmental public body and

agency, and indeed many functions of the BBC and Channel 4 as public broadcasters. Then there are 270,000 data controllers - organisations processing personal information across the private, public and voluntary sectors. There is also common ground in the sense that we live in the “Century of Information” and common ground in that both sets of regulation recognise that there are competing public interests, which can be very controversial at times. To illustrate from my diary today, I have been involved in a meeting with the Chief Executive of the NHS about electronic health records which raised issues about the distinction between elective surgery and emergency treatment, a meeting with a Minister on the possible sharing of data about social security claimants for school dinner purposes, a freedom of information case about the Iraq invasion and a meeting about some missing data discs. Life is never dull! Both freedom of information and data protection very much concerned with social, cultural and democratic values. The focus of the Centre of Regulated Industries is perhaps more usually directed at economic issues. But questions of economics can sometimes intrude into our area, both in relation to substantive cases (especially where commercial interests are involved) but also, for example, harnessing the power of markets to achieve our statutory objectives .

The re is further common ground in that, historically at least, there has been quite a lot of ignorance, undervaluation, scepticism and perhaps hostility. There has been a reluctance to recognise the significance of data protection, often dismissing it to the margins. Likewise, freedom of information has been as a somewhat strange or alien beast, with many not knowing quite how to relate to it. So sometimes we have faced an uphill battle in getting our responsibilities taken seriously. But times have changed over the last 5 years – and very rapidly in the last month or so in relation to data

security – so that both official and personal information are increasingly seen as valuable assets held by all organisation, which need to be treated with the care and respect afforded to other types of asset.

Despite the similarities, I recognise that there are differences and perhaps tensions between freedom of information and data protection. Data protection is fundamentally concerned with confidentiality and the protection of information and (as I indicated earlier) has very strong European origins. Fol is much more about openness and transparency. Sometime culturally it is difficult for any organisation to be protective of information and to be open at the same time, and it can sometimes be difficult for my office as the regulator to strike the right balance between two apparently competing cultural approaches. But the approaches can be reconciled in the sense that one area of regulation safeguards *personal* information and the other seeks greater transparency for *official* information. Section 40 of the Freedom of Information Act dovetails and reconciles the two approaches. To summarise that complex section, information is not disclosable under the Freedom of Information Act if it is personal data and the disclosure of that personal data would breach one of the Data Protection Principles. As the Commissioner responsible for both Acts I believe that I am well-placed to ensure that both strands of public policy are fully ventilated and balanced in those difficult cases where public disclosure may unduly threaten individual privacy.

There is much common ground and some scope for tension. We reconcile the two strands with the ICO the mission which simply describes us as **‘Promoting public access to official information and protecting your personal information’**.

Freedom of Information – rights and rationales

I turn now to say more about freedom of information, assuming some familiarity with the way that the legislation works. There are some 70 countries around the world with Fol legislation, or access to information of one sort or another, and our approach is broadly parallel to that found in many other countries. The UK law was enacted in 2000 after a white paper in 1997, having regularly appeared on various manifestos for many years before that. Most of the Act did not come into force until 2005. The 'right to know' - promoting transparent and open government - in effect provides that there is a presumption of disclosure of all official information unless there are good reasons for secrecy. The Act provides that "any person" may make a request to any public authority, which then has a duty to fulfil a legitimate request unless an exemption comes into play to justify non-disclosure. There are some 23 different exemptions. A public interest test applies to most of the exemptions – described as "qualified", which means the information must still be disclosed unless the public interest in maintaining the exemption outweighs the public interest in disclosure. There were those, when the legislation was first enacted, who claimed that, with so many exemptions, the legislation was going to be a damp squib with nothing changing. They were wrong. There were also those who said Fol is a fundamental challenge to public administration and that good government would not survive. Such sceptics claimed that good government and open government could not co-exist. They echoed, perhaps, the very first 'Yes Minister' programme when the mythical Cabinet Secretary took for granted that "You can be open or you can have government". Those modern-day Sir Humphries have also been proved wrong. At the same time, I am the first to acknowledge that Fol does amount to a major

challenge to a culture of unnecessary official secrecy and our job involves tackling that need for cultural change head on.

This is helped by articulating the rationales for greater openness which are hard to resist. They include increased accountability (for policies, for operational activities and for public expenditure), deterrence against corruption, impropriety, maladministration and bad government, and improving the quality of decision making. This latter point is more controversial - the possibility of disclosure, it is said, will improve the quality of decision making if advisers and politicians know that their advice, their analysis, their facts, their figures, their statistics are (or may be) open to public scrutiny. They will be that much more careful and objective if they know that wrong, misguided or inappropriate considerations may well be made public at some stage.

In New Zealand, the open government law has just celebrated its 25th anniversary. Open government is now largely embedded in the political culture. A great deal of advice is now routinely made available at the time it is given. Borrowing from a more economic analysis, theories of contestability are now deployed. It is said there is now less of a monopoly of wisdom inside the government system. Advice, analysis and decisions more regularly have to withstand external scrutiny and the possibility or fact of competing approaches. This is especially the case for second-order matters - not the most highly controversial issues - where materials are there for public scrutiny on websites. Outsiders can comment on matters even before decisions are made. Such openness has not yet arrived in this country, but we are gradually moving in that direction.

FoI is also rationalised in terms of building public trust and confidence and reinforcing democratic values. It brings knowledge to the people, serving as a reminder that in, a democracy, politicians, officials are acting in the name of the people, with the people's money and on behalf of the people. It is a reminder of that value, with considerable legitimacy for those who say that an access regime is fast becoming a defining characteristic of a modern democracy.

I was delighted when on 25th October 2007 the Prime Minister in his speech on "Liberty" recognised these points. This was a very wide ranging speech, analysing concepts of Liberty in the language of history, philosophy and political science and then moving on to specific reforms. The Prime Minister described freedom of information law as a "landmark piece of legislation". He went on to say that it could be

"...inconvenient, at times frustrating and indeed embarrassing for governments. But FoI is the right course because government belongs to the people....There is more we can do to change the culture and workings of government to make it 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. Wherever possible that should be the guiding principle behind the implementation of our Freedom of Information Act."

Given that our regulatory challenge involves so much culture change – which always has to be led from the top – it is very welcome to have such sentiments expressed by the Prime Minister. I believe these remarks are being taken very seriously across the public sector.

Of course there are fears that greater openness will damage the candour and frank advice needed inside government and all other organisations. I addressed these concerns at length in a speech in September entitled ‘Open government is good government’. I reviewed the impact of FoI mainly on the areas of central government policy making where exemptions relating to the formulation of government policy and the effective conduct of public affairs most frequently come into play. I analysed in greater detail how the law is being applied in this area. I tried to make the case – recognising that it is not a black and white case - that the trends towards more open government are indeed trends towards good government. I pointed out that we are very aware of the arguments about the so-called “chilling effect” with the possibility of disclosure having an inhibiting effect on what is said, written down, or recorded. We are sensitive to that argument in particular situations, but we are less tolerant of it where entirely innocuous material is withheld because of a possible chilling effect. However where there is genuinely sensitive material we have been at pains to recognise the damage which could be done if that was to be disclosed prematurely.

Freedom of Information – Three Years of Experience

The new law has now passed its third anniversary. It is now common place that there are daily disclosures in the national, regional and local media which are labelled as “disclosed under the Freedom of Information Act”. It is now routine to see information coming into the public domain, either proactively or in response to requests. It is now part of the fabric of public life. Having said that, there has been a very steep learning curve for all concerned and a great deal of boundary testing. It was perhaps a mistake to adopt a “big bang” approach where the entire Act came into force for all public authorities on the same day. There was no piloting. There was no gradual implementation. So everyone entered the deep end at the same time – with challenges for public authorities, for requesters and indeed my own office. A great deal of boundary testing still continues on the part of both requesters and on the part of public authorities.

Annual reports and other materials from my office bear out a generally positive response from public authorities. We regularly appeal to their sense of enlightened self interest. We pointed out how many public sector websites proudly proclaimed their commitment as a transparent body with open values. The Act is a test of that in reality. Most public bodies are passing the test of commitment, at least in terms of effort. True, there has been some recalcitrance and some lack of enthusiasm, but this not an overwhelming position. There is now a recognition that legislation is irreversible and a determination on the vast majority of politicians and public servants to make the best of the law and to take it seriously.

There has certainly been a strong public appetite for using the right to know, with high volumes of requests. The Ministry of Justice reports statistics for central

government departments and extrapolating from that, with our own figures of complaints, we estimate there have been at least 200,000 - and probably closer to 300,000 - requests made over the first 3 year period. The majority of requests are granted either in full or in part without coming anywhere near my office. Although we have had more than 7,000 complaints in 3 years that is actually quite a small number compared to 300,000 requests. This suggests that – despite considerable concerns about delay at all stages – the law is generally working reasonably well. We have closed over 6,000 cases including over 750 formal decision notices, all of which are published on our website. Each decision notice has to set out a full analysis of the complaint in each case - the facts, the law and public interest judgements as appropriate - either upholding the complaint or rejecting it, or sometimes finding some middle ground. Decisions very rarely run to less than 10 pages and sometimes can take as much as 20 or 30 pages. We have to analyse the individual circumstances of each case across an extraordinarily wide range of subject matter. We have real teeth - we can order the public authority to disclose information where appropriate and (in the absence of a successful appeal) it is contempt of court not to obey one of our decision notices.

We have very limited resources - only £4.7 million for the entirety of our work right across all freedom of information activity for the current year. We are hoping for more as we move forward into next year because we have had backlog problems, although we are closing 55% of the more straightforward cases within a month. But those cases which do need a full investigation typically have to wait 6 months before we can even start an investigation. I don't find that acceptable. I find it wrong that a case has to wait 6 months before we can get properly started. I hope that it is not

arrogant to claim wide respect for our decisions. Many of them are complex and controversial, but the fact that less than a third are appealed to the Information Tribunal is an encouraging indicator of quality. Either side, requester or public body, can appeal - it is virtually risk free, it is largely cost free. What is more, we find that our overall approach is supported in about three quarters of the appeals which get to a hearing.

Our Annual Report for 2006-7 documented that just over 45% of cases in that year were resolved informally. In just over 12% of cases there was a formal decision notice. In terms of outcome, we upheld the complaint in about 26% of cases, we did not uphold 39% and in 35% we varied the public authority's response, upholding part of the complaint but not the totality. Last year a total of 92 cases were appealed to the Information Tribunal.

To give a flavour of variety of subject matter, these have included toxic waste, speed cameras, the expenses of Members of Parliament (a topic of continuing controversy), local authority pension investments in hedge funds, the contract between Ryanair and Londonderry Airport (a case calling for strong economic analysis and State Aid considerations), the scrutiny of the identity cards programme, airport noise data, the 1911 census, the location of possible prostitution zones in Liverpool, and ministerial advice on angling. The case where we ordered the Treasury to disclose the advice to the then Chancellor in 1997 which led to changes in the taxation regime for dividends and its impact on pension funds was a very controversial and difficult decision. We made what we thought was the right decision. The Treasury appealed, but then withdrew their appeal and the information

was disclosed. It was not a comfortable time for the Chancellor, perhaps made worse by the impression that the information had to be pulled into the public domain by a long drawn out and difficult process. This may have been more troublesome in political terms than disclosing the information in the first place.

Many cases relate to the spending of public money, for example

- the Wells Report into the NHS University
- the highest paid barristers in legal aid
- university investments in arms companies
- road damage compensation claims
- cost of police merger plans
- police spending on hire vehicles
- councils' spending on agency and temporary staff
- CSA Computer system costs

It is inevitable that decisions which go against the will of the public authority tend to get more publicity and more awareness. But in many cases we uphold the position of the public authority in refusing disclosure, such as various “live” policy issues, access to deceased patient records, compensation payments which would identify individuals, files relating to the prosecution of Jeremy Thorpe some 28 years ago, details of a very acrimonious dispute between the Foreign Office and the Foreign Press Association, vexatious requests such as more than 100 requests about an allotment site to Birmingham City Council, and commercially sensitive information held by the Post Office.

How do the public view greater openness? We conduct a survey every year to explore public attitudes towards the benefits of freedom of information. It is a longitudinal study asking exactly the same question of a sample of the general population over the last 4 years.

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



The shifts towards positive reaction have been marked. We are proud that we have enforced this law in a responsible robust way and that the benefits are manifestly and increasingly seen by the general public.

To conclude on this aspect, we believe FoI is working well - but there are challenges for my Office and there is still more to do in terms of accelerating the pace of cultural change across the public sector. At the same time we recognise the importance of identifying and demonstrating those situations where secrecy is necessary. We continue to push the theme of enlightened self interest articulating the benefits of openness to public authorities and the dis-benefits of secrecy or resistance.

Over time, as mentioned earlier, we see a gradual shifting away from one off

requests and complaints, much more down the road of improving compliance in the first place and securing routine proactive disclosure on the part of public authorities.

Data Protection

I switch now to data protection and start by recognising data protection has had a somewhat mixed reputation. It has, as I mentioned earlier, a strong European heritage and requires an understanding of the legacy of the Nazis and Soviets in 20th Century Europe. The driving force for data protection came from Germany in the 1950s and spread to other parts of Europe. It came to the UK rather later than elsewhere. The European Directive was finally adopted in 1995. In my view the Directive itself is problematic – it lacks clear objectives and is somewhat out-dated. It was conceived at a time when there were only a handful of mainframe computers. The Lindop Committee's Report listed every computer in this country showing how far we have come since the origins of data protection were put in place.

The Directive is also excessively bureaucratic. It is very much focused on process, with silence about the outcomes it is trying to secure. It is a rather old fashioned piece of legislation in terms of good regulatory theory. It is not well drafted, with a mix of general principle and some very detailed prescription. There is no obvious or clear strategy of self-enforcement, nor a programme of incentives or sanctions for compliance. The UK Act was transposed in the late 90s with a certain amount of gold plating.

Although I am critical of much of the legislative infrastructure, the key Data Protection Principles are expressed in clear language and are of fundamental importance. The rationales are about establishing privacy and respect for the integrity of personal information. The Principles require personal information to be processed lawfully and fairly and for limited purposes. Such information must be adequate, relevant and not excessive. It must be accurate and up to date and not kept longer than is necessary. And there must be appropriate standards of security.

A Strategic approach to Data Protection in practice

These are not controversial principles –though sometimes their application can be difficult - but there is no serious challenge to the underlying rationales. In the 5 years that I have been Commissioner I have summarised our approach as **“taking a practical down to earth approach, seeking to simplify for the majority who try to handle personal information well and to be tougher for the minority who do not.”** With this approach we combine the role of influencer, promoter and enforcer. We have published a plethora of good practice notes in recent years, setting out the Do’s and the Don’ts for organisations expressed in very clear language which have been well received. We also give advice to the general public - we have a very busy helpline, our website gets over 1.5 million hits every year and there is certainly a public demand to know where they stand in this area. We get more than 25,000 specific enquiries and complaints. Most of these are matters concerning direct personal concerns. Most are fairly straightforward to resolve - either misconceived or involving some ignorance or lack of awareness on the part of the organisation concerned.

With enforcement activity we have changed our complete philosophy. With a theme of “Selective to be Effective” we have put in place an Enforcement Strategy which sets out the criteria for identifying those cases now where we carry out an investigation with a view to possible use of our enforcement powers. Such cases often involve deliberate or persistent non-compliance or high profile example cases which can clearly bring a therapeutic benefits.

More generally, we have produced a draft **Data Protection Strategy** document for our data protection work as a whole, articulating the objectives and strategy which is (at best) only implicit in the legislation. There has been considerable interest in Europe and more widely internationally in the approach we are taking, especially the need for maximum focus and selection. Our strategy places considerable emphasis on protecting people, rather than more abstract notions of data protection. It spells out the importance of building public confidence, simplifying and being pragmatic, communicating effectively and influentially, working wherever possible constructively in partnership with others, avoiding a paternalistic approach, minimising the burdens on organisations, harnessing market and political forces and appealing to enlightened self interest.

A very strong theme is to take a risk based approach - setting as our goal respect for personal information through organisations meeting reasonable expectations of integrity, security and fairness in the collection of and use of information. This involves, with all the main issues, analysis of the potential risks of detriment to individuals or to society. It means assessing the seriousness of the detriment and the likelihood that it will materialise. The criteria in our strategy inform our approach to

setting priorities, selecting issues, defining outcomes and testing that we are using our resources to best possible effect. The strategy, codifying our progress over recent years, gives us the authoritative and influential voice which all regulators must seek.

Data Protection Issues

There are many examples where we have sought to be influential in our work. We have done a lot of work pointing out the extent to which this country is sleepwalking into - or perhaps waking up in - a surveillance society. We commissioned a major report in November 2006 from the Surveillance Studies Network documenting the nature and the extent of the huge amount of information now being collected by public and private sector organisations. It set out how database growth leads to the electronic footprint which each of us leaves now in our daily lives. It pointed out what is currently happening and then projected forward over the next 10 years based on documented proposals, initiatives and trials. The report was launched at the International Data Protection Commissioners' Conference which we hosted in London. The report made clear that these developments have not arisen from any ill intent. There is no sinister plot to monitor the entire population, still less any sort of autocratic state.

There was a lot of media and political coverage of the issues. There are now two Select Committees - one in the House of Commons and one in the House of Lords - looking at the issues raised in that report. They are complicated, with competing public policy considerations. We do not have magic answers, but we are putting

these forward for debate for discussion and to have a fuller debate than we have so far had about the explosion of personal data collection.

Part of the Act says that I am entitled to make a report to Parliament on a matter of particular interest and I did so for the first time in our 20 year history in 2006 with a report entitled 'What Price Privacy?'. This followed some frustrating prosecutions we had brought and it documented a pernicious and illegal trade in personal information. This has been a criminal offence since the early 1990's with very weak penalties. Some major cases we have taken to the courts have resulted in fines of just £100 - £200 or less. One major case resulted in conditional discharges for all concerned. The main technique is known as "blagging" with people able to access databases and get through call centres by impersonating individuals. We were able to obtain some of the training manuals of private detectives involved in this trade. We have got tape recordings of their activities. We have got invoices from a range of organisations paying for these services - not just the tabloid press, but also law firms, insurance companies, banks and others paying private detectives in order to get information which surely should have been kept confidential right from the outset. We have had some very positive responses from bodies such as the Office of Fair Trading, the Financial Services Authority, the Security Industry Authority, and the Law Society. They all took measures we recommended to tighten up on this activity to make clear it is not acceptable.

A less positive response was received from the newspaper world, but we are now working constructively with the Press Complaints Commission. And of course we are delighted that the government has agreed that the penalty for the criminal offence

should be increased. The Criminal Justice and Immigration Bill, currently going through Parliament, increases the penalty exactly in line with our recommendation which is a prison sentence to act as a deterrent - 6 months for a summary trial and two years on indictment. We hope that the Bill will swiftly go through to Royal Assent and we hope that will certainly send a very clear message to all concerned this sort of behaviour is totally unacceptable.

We make a contribution on a wide range of other matters. On the controversial area of identity cards, but our primary concern has always been with the National Identity Register – the database behind the cards. In particular, we have strong worries about proposals for transactional information – details of daily card use – to be held on the register. We have engaged with the Department for Children, Schools and Families (the former DfES) on ContactPoint, the Children's Index - an index on every child in the country from birth up until age 18. We have questioned the rationale for that, but also the arrangements for collecting the data and how it is to be kept secure, accurate and up to date. Electronic health records raise major issues. The Connecting for Health project is the largest civil IT scheme in the world with many implications. We have had discussions with the National Health Service on that. Obviously security is of a particular concern, but accuracy (ensuring no patient mis-matches) and keeping care records up to date are just as important.

Privacy Impact Assessments

We are having a very constructive debate with the Department for Transport on privacy and security implications of road user charging. There are various ways in which you can track vehicle movements - some less privacy intrusive than others.

We are particularly pleased that they are prepared in principle to test the concept of a Privacy Impact Assessment. We have put forward detailed proposals for using PIAs. In December 2007 we launched our interactive PIA Handbook, setting out how to undertake an assessment of the privacy implications of a new initiative. We want to see the PIA approach used, not on a mandatory basis, but as a matter of good practice by organisations **before** embarking on a programme of collecting or sharing personal information on any major scale. The PIA technology has been widely used in other parts of the world. We have developed a UK application and are pleased there have already been many positive reactions.

CCTV and Data sharing

CCTV cameras have been one focus of our surveillance work. There are more cameras per head of population in this country than anywhere else in the world. We published a Code of Practice over 5 years ago, but it has become somewhat out of date. We are launching a new edition of the Code of Practice, which has followed extensive consultation, at the end of January. This takes account of new technologies, such as facial recognition, and takes a strong stand against the use of microphones with CCTV cameras.

Data sharing is a controversial and difficult subject and here we have also published a Framework Code of Practice for the sharing of personal information. The framework code gives a standard template for use by all organisations needing or wanting to share information. It provides a controlled way for them to elaborate their own codes of practice tailored for their particular purpose. The Review of Data

Sharing which the Prime Minister has asked me to conduct with Dr Mark Walport of the Wellcome Trust will clearly probe data-sharing issues in greater depth.

Data Security Breaches

When we launched the Annual Report in July 2007, I used strong language about inexcusable security breaches involving personal data. I used the language of a “frankly horrifying roll call” of security breaches we had come across - involving clearing banks, retailers, public bodies and others. We gave examples of laptops being taken out of an office containing large amounts of personal information where there had not been proper encryption; of large volumes of credit card transactions falling into the wrong hands; of problems with doctors’ on-line recruitment and visa applications, where people were able to see the circumstances of others. There was inadequate security on websites in those cases, but it was the large number of banks had been careless with paper records which attracted substantial media attention. Banks had dumping very sensitive financial information (such as bank statements, funds transfers, loan and insurance applications) in rubbish bags in places easily accessible to the general public. These related to identifiable individuals, with names account numbers and other details. We took a very poor view of that and in late 2006 and we secured Undertakings which we asked the Chairman or the Chief Executive of each of the clearing banks to sign personally. This was to make sure that the issues were being taken seriously. The undertakings related to future good practice. Also, given that we do not have the power to inspect an organisation without its consent, each of those undertakings included consent for us to carry out future inspections. We have since inspected 4 or 5 banks on physical security over the

recent months and I have to say they have all improved their performance quite dramatically.

In our report we spelt out that good security and good data protection are not just matters of enforcement and compliance with the law. It involves losing the trust and confidence of your customers, your citizens, your staff, your employees, and others you deal with. It directly involves reputational damage. We called for a “wake up call” on the part of business and public sector leaders to take information rights seriously. Our report in July said this should be on the agenda of every Chief Executive and every Permanent Secretary.

The more recent security breaches involving government departments and other public bodies have certainly left no doubt that the wake up call has now been heard. The landscape has changed in the last couple of months. With HMRC and the 25 million sets of missing child benefit details, there was astonishment that so much data could be copied on to 2 discs. An enquiry is now in progress, but there are searching questions to be answered in terms of policies, procedures and actual behaviours. Other cases have involved the Driving Standards Agency, the National Health Service (and of course more cases have come to light since the date of this lecture).

There is at last a recognition that there needs to be much more seriousness towards data protection. I am very pleased that the Prime Minister and the Cabinet Secretary have sent some very encouraging signals on this front. It now seems recognised that my Office need proper inspection powers. There is now a commitment of

government policy that we can inspect public bodies without the consent of the organisation having first to be obtained. There is also a commitment to introduce new sanctions for the more serious cases. I am optimistic that there is also a recognition that we need more resources to undertake new responsibilities as we move forward. Watch this space!

Conclusion

We are living in a very fast-changing environment. The pace of change has accelerated dramatically over the last 2 or 3 months, but it has been part of a trend to take information rights a great deal more seriously in recent years. A sea change is sweeping the world of information rights. The issues raised by privacy, data protection, freedom of information are at last seen as highly relevant, topical and not just on the margins. They are setting part of the national agenda in various ways. There has been over the last 2 or 3 years very extensive parliamentary and public discussion. Although freedom of information was a new and strange creature when it arrived, it is clear now that it is here to stay with its central themes now irreversible.

Data protection and privacy have come of age. This has been a long time coming but we have moved away from an almost theological or academic approach to data protection. Now we have succeeded in making it much more focused on the realities of life for private citizens. But we must not be complacent. We still need some renewal. I shall be announcing shortly a project to examine what is right and what is wrong with the European Directive and from that in due course may flow changes to the UK legislation. Changes may also flow from the Data Sharing Review I mentioned earlier.

Across all the subject matters affected by information rights there is now much greater awareness of the risks of getting things wrong and also the benefits of getting things right. There is a recognition of the need for focus on the fundamentals in this area which are ultimately those of **governance** and **accountability**, establishing exactly who is responsible for what and making absolutely clear where responsibility for information duties lie and making sure they are achieved in practice.

I have covered only domestic matters in this lecture, but this is a global agenda. Information now flows internationally regardless of geographic borders. We have much dialogue and debate with our counterparts in Europe, in the United States, in Australasia, in South East Asia and elsewhere. This has to be part of a convergence of approach. There are some major challenges as legislation and cultures are very different in different parts of the world. But in my view a far more converged approach is as inevitable as it is desirable.

I have shared some insights into our regulatory approach, style and achievements. Above all, we strive to be effective. We have plenty of challenges ahead. The work is demanding, but stimulating. I was pleased to be re-appointed for a further 2 years, but I hope that when I leave in June 2009 my office will be in very good shape to take on even more new challenges as we move forward.

Richard Thomas