Data Sharing Review

Richard Thomas and Mark Walport

Data Sharing Review Report

11 July 2008

Foreword

Dear Prime Minister and Secretary of State for Justice

We are pleased to present our report on Data Sharing. As recent events have shown, this is a topic that is timely, important and a matter of great public interest and concern. We have consulted widely in order to inform our thinking. Decisions about the extent of data sharing go to the heart of the fundamental democratic debate about the relationship between individuals and society. There is a long-standing and healthy debate about the balance between the right of individuals to privacy and the necessity for the state to hold personal information about citizens. Government uses personal information for purposes such as providing the fundamental democratic right to vote, the collection of taxes, protection of citizens and provision of services. But there are limits to the extent and purposes for which Government should use personal information about citizens. This report examines how these limits should be set.

It is impossible to take a generic view of data sharing. Data sharing in and of itself is neither good nor bad. There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data. Data sharing needs to be examined in specific terms. Is the sharing of particular elements of personal information for a defined purpose in a precise fashion, likely to bring benefits that outweigh significantly any potential harm that might be associated with the sharing?

There are two key steps in the implementation of any scheme to share personal data. The first is to decide whether it is appropriate to share personal data for a particular purpose. The second is to determine how data should be shared, in particular what and how much data, and by what means.

There can be no formulaic answer as to whether or not it is appropriate to share personal information. The legal context for the sharing of personal information is encompassed by the common law, the European Union Data Protection Directive, the Data Protection Act and the Human Rights Act. We have found that in the vast majority of cases, the law itself does not provide a barrier to the sharing of personal data. However, the complexity of the law, amplified by a plethora of guidance, leaves those who may wish to share data in a fog of confusion.

Repeated losses of sensitive personal information in both the public and private sectors demonstrate the weakness of many organisations in managing how data are shared. The advent of large computer databases has allowed the loss of massive datasets in ways that were simply impossible with paper records.

We make recommendations that should improve decision making about the circumstances in which personal data may be shared and that will also improve the means by which data are shared.

Our most important recommendation calls for a significant improvement in the personal and organisational culture of those who collect, manage and share personal data. In the last few decades there has been a major improvement in governance in the commercial, charity and voluntary sectors. However, in many organisations the governance of the

handling of personal information has not followed suit. We recommend that rigorous training of those responsible and accountable for the handling of personal information, backed-up by enhanced professional development, accountability, reporting and audit, will effect a major improvement in the handling and sharing of data.

A strong regulator is also needed to facilitate these cultural improvements. It is essential that the regulator has sufficiently robust powers and sanctions available to it; and that it is resourced adequately. We welcome recent changes in the law to provide the Information Commissioner with a power to impose financial penalties for wilful and reckless breach of the data protection principles and call on the Government to implement these changes quickly. We also believe that stronger inspection and audit powers are required and that new funding arrangements to enable effective enforcement are long overdue. We also recommend an important change in the nature of the office of the Information Commissioner in order to improve the provision of guidance and the regulatory oversight of the handling and sharing of personal information. We recommend that a Commission with a supporting executive team replace the single Information Commissioner.

There should be a statutory duty on the Commission to provide a code of practice for the sharing of personal information to remove the fog of confusion about the circumstances in which personal data may be shared. Where there is a statutory bar to the sharing of personal information, we recommend a fast-track legislative framework that will enable transparent Parliamentary consideration as to whether the bar should be removed for particular purposes. Public policy needs to be based on the strongest possible evidence, which requires research and statistical analysis. We make recommendations that will enable such research and statistical analysis to be undertaken in a way that provides the maximum protection to the privacy of individuals.

None of this is a substitute for good judgement and common sense, which are key to making wise decisions about whether or not to share personal data. It is equally important that such decisions are taken in the context of good mechanisms of governance including transparency, audit and accountability. This approach will allow individuals and society to secure the many benefits that flow from the appropriate sharing of personal information, while avoiding and minimising the potentially serious harm that inappropriate sharing or mishandling of precious personal information may cause.

We look forward to the response of the Government to our recommendations, with a timetable for their implementation. We would appreciate in addition a progress report from Government in eighteen months time. We thank you for asking us to undertake this fascinating and challenging review.

Richard Thomas and Mark Walport

Contents

Executive Summary

1. In his Liberty speech on 25 October 2007 the Prime Minister announced that he had asked us (Mark Walport and Richard Thomas) to undertake a review of the framework for the use of personal information in the public and private sectors.

2. The terms of reference asked us to consider whether changes are needed to the operation of the Data Protection Act 1998; to provide recommendations on the powers and sanctions available to the Information Commission and the courts in the legislation governing data sharing and data protection; and to provide recommendations on how data-sharing policy should be developed to ensure proper transparency, scrutiny and accountability. Our terms of reference are set out in full in *Annex A*, published alongside our main report.

3. In the light of these terms of reference, we have focused primarily on the issues surrounding the sharing of personal information that have given rise to recent problems and anxieties: how is data shared? by whom? with what authority? for what purposes? with what protections and safeguards? We have further considered what changes to data protection laws and practice might improve the current situation. This focus became altogether more apposite just a few weeks after our appointment, when Her Majesty's Revenue and Customs announced that it had lost two disks containing personal information of some 25 million people.

4. We begin by briefly setting out the context of the current debate in Chapter 1. In Chapter 2 we set out a simple taxonomy that describes the vast majority of valid reasons for sharing personal information: law enforcement and public protection, service provision and delivery, and research and statistical work.

5. In Chapter 3 we set out the key elements of the complex legal framework that currently governs data sharing. It is clear that the framework as it stands is deeply confusing and that many practitioners who make decisions on a daily basis about whether or not to share personal information do so in a climate of considerable uncertainty.

6. After drawing attention in Chapter 4 to the critical importance of public trust and confidence in organisations' handling and sharing of personal information, we move on to review in Chapters 5 and 6 the principal factors that impact on whether and how personal information should be shared, and the landscape within which such sharing may take place. For this we draw on our extensive consultation. Questions of consent arouse considerable passions. Much could be done to distinguish more clearly between genuine consent and consent that is simply enforced agreement. In considering questions about the sharing of data, however, the central point is one of proportionality – when is it proportionate to use or share data? This is central to our report and the question that must be kept in mind at all times. We further discuss the legal ambiguity within which people commonly work, and the need for clear guidance, professional skills and rigorous training in matters of personal information.

7. High levels of accountability and transparency are vital to the way organisations handle and share personal information, yet these are all too often absent. People working within organisations will often not know who is responsible for data-handling matters, nor whether any particular individual will be held accountable if things go wrong. People at large are, as a rule, given little insight into how their personal information is used and shared by organisations that hold it, and have even less knowledge of the organisations with which their information is shared. Action is needed on both these fronts. Technology has had a huge impact on the ways in which data are handled. It has enabled the creation of large and easily accessible databases and has provided both increased levels of security and increased risks of large-scale data breaches. It is important that people do not find themselves led simply by what technology can achieve – they need to understand first of all what they want to achieve.

8. In Chapter 7 we consider the existing powers and resources available to the Information Commissioner. There is strong evidence that his bite needs sharpening and that increased funding is required for him to carry out his duties. We make recommendations to those ends in the following chapter, as well as a recommendation to change the structure of the existing office of the Information Commissioner.

9. In Chapter 8 we make a series of detailed recommendations, summarised below. Some of these recommendations require legislative change while others do not. We look to the Government and to the wider public and private sectors to take on these proposals, which we believe will lead to improvements in the governance and understanding of data sharing. We also look to individuals themselves to take responsibility for the way in which they protect their personal information. This information is individual and precious to each one of us, and we should all play a part in keeping it safe.

Recommendations

10. Based on the evidence we have collected and analysed, we believe change is necessary to transform the *culture* that influences how personal information is viewed and handled; to clarify and simplify the *legal framework* governing data sharing; to enhance the effectiveness of the *regulatory body* that polices data sharing; to assist important work in the field of *research* and statistical analysis; and to help safeguard and protect personal information held in publicly available sources.

11. Our recommendations, in summary, are:

Developing culture

***Recommendation 1*:** As a matter of good practice, all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information.

Recommendation 2: As a matter of best practice, companies should review at least annually their systems of internal controls over using and sharing personal information; and they should report to shareholders that they have done so.

Recommendation 3: Organisations should take the following good-practice steps to increase transparency:

(a) Fair Processing Notices should be much more prominent in organisations' literature, both printed and online, and be written in plain English. The term 'Fair Processing Notice' is itself obscure and unhelpful, and we recommend that it is changed to 'Privacy Policy'.

(b) Privacy Policies should state what personal information organisations hold, why they hold it, how they use it, who can access it, with whom they share it, and for how long they retain it.

(c) Public bodies should publish and maintain details of their data-sharing practices and schemes, and should record their commitment to do this within the publication schemes that they are required to publish under the Freedom of Information Act.

(d) Organisations should publish and regularly update a list of those organisations with which they share, exchange, or to which they sell, personal information, including 'selected third parties'.

(e) Organisations should use clear language when asking people to opt in or out of agreements to share their personal information by ticking boxes on forms.

(f) Organisations should do all they can (including making better use of technology) to enable people to inspect, correct and update their own information – whether online or otherwise.

Recommendation 4: All organisations routinely using and sharing personal information should review and enhance the training that they give to their staff on how they should handle such information.

Recommendation 5: Organisations should wherever possible use authenticating credentials as a means of providing services and in doing so avoid collecting unnecessary personal information.

The legal framework

Recommendation 6: Any changes to the EU Directive will eventually require changes to the UK's Data Protection Act. We recognise that this may still be some years away, but we nonetheless *recommend* strongly that the Government participates actively and constructively in current and prospective European Directive reviews, and assumes a leadership role in promoting reform of European data law.

Recommendation 7(a): New primary legislation should place a statutory duty on the Information Commissioner to publish (after consultation) and periodically update a data-sharing code of practice. This should set the benchmark for guidance standards.

Recommendation 7(b): The new legislation should also provide for the Commissioner to endorse context-specific guidance that elaborates the general code in a consistent way.

Recommendation 8(a): Where there is a genuine case for removing or modifying an existing legal barrier to data sharing, a new statutory fast-track procedure should be created. Primary legislation should provide the Secretary of State, in precisely defined circumstances, with a power by Order, subject to the affirmative resolution procedure in both Houses, to remove or modify any legal barrier to data sharing by:

- repealing or amending other primary legislation;
- changing any other rule of law (for example, the application of the common law of confidentiality to defined circumstances); or
- creating a new power to share information where that power is currently absent.

Recommendation 8(b): Before the Secretary of State lays any draft Order before each House of Parliament, it should be necessary to obtain an opinion from the Information Commissioner as to the compatibility of the proposed sharing arrangement with data protection requirements.

The regulatory body

Recommendation 9: The regulations under section 55A of the Data Protection Act setting out the maximum level of penalties should mirror the existing sanctions available to the Financial Services Authority, setting high, but proportionate, maxima related to turnover.

Recommendation 10: The Government should bring the new fine provisions fully into force within six months of Royal Assent of the Criminal Justice & Immigration Act, that is, by 8 November 2008.

Recommendation 11: We believe that as a matter of good practice, organisations should notify the Information Commissioner when a significant data breach occurs. We do not propose this as a mandatory requirement, but in cases involving the likelihood of substantial damage or distress, we *recommend* the Commissioner should take into account any failure to notify when deciding what, if any, penalties to set for a data breach.

Recommendation 12: The Information Commissioner should have a statutory power to gain entry to relevant premises to carry out an inspection, with a corresponding duty on the organisation to co-operate and supply any necessary information. Where entry or co-operation is refused, the Commissioner should be required to seek a court order.

Recommendation 13: Changes should be made to the notification fee through the introduction of a multi-tiered system to ensure that the regulator receives a significantly higher level of funding to carry out his statutory data-protection duties.

Recommendation 14: The regulatory body should be re-constituted as a multi-member Information Commission, to reinforce its status as a corporate body.

Research and statistical analysis

Recommendation 15: 'Safe havens' should be developed as an environment for population-based research and statistical analysis in which the risk of identifying individuals is minimised; and furthermore we *recommend* that a system of approving or accrediting researchers who meet the relevant criteria to work within those safe havens is established. We think that implementation of this recommendation will require legislation, following the precedent of the Statistics and Registration Service Act 2007. This will ensure that researchers working in 'safe havens' are bound by a strict code, preventing disclosure of any personally identifying information, and providing criminal sanctions in case of breach of confidentiality.

Recommendation 16: Government departments and others wishing to develop, share and hold datasets for research and statistical purposes should work with academic and other partners to set up safe havens.

Recommendation 17: The NHS should develop a system to allow approved researchers to work with healthcare providers to identify potential patients, who may then be approached to take part in clinical studies for which consent is needed.

Safeguarding and protecting publicly available information

Recommendation 18: The Government should commission a specific enquiry into on-line services that aggregate personal information, considering their scope, their implications and their regulation.

Recommendation 19: The Government should remove the provision allowing the sale of the edited electoral register. The edited register would therefore no longer serve any purpose and so should be abolished. This would not affect the sale of the full register to political parties or to credit reference agencies.

12. We strongly commend these recommendations to the Government and we look forward to a timely response. In particular we would like the Government, as part of its response, to set out a clear timetable for implementation and to report on progress in eighteen months time.

1. The context of the review

1.1 Personal information – about our identities, characteristics, activities, opinions and all other aspects of our lives – defines each of us as individuals and as members of society. This review is about the use of that information[1]. Personal information can be used to enrich our lives, but it can also be misused in a way that controls and condemns us.

1.2 The development of an information society reliant on databases has resulted in the continued growth of extensive personal datasets. This information is collected by others – public, private and third-sector organisations – for understandable motives. The state offers security to citizens by enforcing the law, protecting the vulnerable and providing public services. Private-sector companies make extensive use of personal information as they market their goods and services, and seek to satisfy our needs and our desires as consumers. Others know increasingly more about us - as employees, as patients, as parents, as children, as taxpayers, as claimants, and sometimes as suspects, law-breakers or victims. There is great scope for personal information to be used for the benefit of individuals and society. But there is also significant scope for abuse, excess and mistakes where the risks and detriments will outweigh the benefits.

1.3 Over recent years, changes in technology enabling more efficient uses of information have transformed and are continuing to transform the public and private sectors. The United Kingdom is now one of the most information-rich countries in the world. Over the past decade, the UK Government and the private sector have invested billions of pounds in public and private-sector IT projects that store and share the personal information of almost every person in the country. The growth of e-commerce through the commercialisation of broadband has resulted in millions of people providing their personal information to others on a daily basis.

1.4 Advances in technology have transformed the ways in which commercial services respond swiftly to consumer demands and preferences. Well-run businesses in a competitive environment know how important it is to earn and retain the confidence of their customers and staff by respecting the information they hold. The public sector has generally lagged behind, both in the technology it deploys and in the priority it gives to establishing strong safeguards. Citizens have increasing expectations that public services will be more responsive and better tailored to their needs. They expect them to be joined up, efficient and user-friendly. But they also have high expectations that their personal information will be kept accurate and fully protected from loss or misuse.

[1] When we use the term *personal information*, we intend to encompass what is meant by section 1 of the Data Protection Act 1998 when it talks of 'personal data', and so in effect about information that relates to a living, identifiable individual. However, we accept that this definition is not without its problems, and we return to this at paragraph *5.25*.

1.5 Society as a whole faces wider challenges, and new technologies bring both opportunities and risks. Citizens throughout the developed world are potentially subject to an unprecedented degree of surveillance. We benefit from mobile telecommunications but at the same time carry personal tracking devices in the form of mobile telephones. Every purchase we make using 'plastic' credit is recorded and shared with the providers of that credit. Our movements in cars, trains and planes are traceable with relative ease. The latest phenomenon of 'social networking' has encouraged millions of people to put personal information onto the internet. But are we aware how our personal data are used now? Who decides when and how to use our personal information? How can we be sure that our personal information is not vulnerable to abuse, now or in the future? And, nearly twenty-five years after the adoption of the broad legislative framework, is the current approach to the regulation of data protection now showing signs of age?

1.6 The abuse of personal information is not in itself a product of the computer and internet age. Paper records have historically provided an effective means for abuse and persecution on a massive scale. The difference lies in the scale, speed of access and sharing, and search efficiency which modern technology brings. Unless they are governed well, misuses of computerised datasets can threaten or cause harm to greater numbers of people in ever shorter periods of time, whether by accident or design.

1.7 It is in this context that we have conducted our review of data sharing. For the purposes of the review, we have adopted an inclusive definition of sharing. This encompasses the disclosure of information about single individuals as well as the more systemic sharing of information about groups of individuals. It is the latter on which we have mainly focused. It also covers the sharing of information within organisations, for example within the NHS between one hospital and another, within Government Departments between one division and another, or in the police between one force and another. It includes sharing between organisations, both small and large. There are important consequences that may arise from the sharing of personal information. Complex social, political, moral and legal questions may arise. The sharing of large datasets can multiply the benefits of data sharing schemes. However, in and of itself, sharing can also amplify the risks and hazards associated with any collection and use of personal information. We present in this review an analysis of the key issues surrounding data sharing in order to provide improved clarity about the scope of sharing of personal information, with the twin aims of promoting beneficial sharing and restricting harmful sharing.

Recent developments

1.8 In recent years, the debate has increasingly shifted from a focus on how personal information is collected to how it is used and shared. The Government has for some time been considering how to facilitate information sharing in order to improve public services and enhance public protection. Two government reports have focused on this: in 2002, *Privacy*

and Data-sharing[2], from the Performance and Innovation Unit; and in 2005, *Transformational Government: enabled by technology*[3], from the e-Government Unit. The following year, the government advisory body, the Council for Science and Technology, published its independent report, *Better use of personal information: opportunities and risks*[4].

1.9 Each of these reports advocated the benefits of sharing personal information more widely by harnessing new technologies. The Council for Science and Technology also made a strong case for putting in place robust safeguards to mitigate the risks that information sharing entails. Recently, the Government published its Vision statement on information sharing[5], articulating its ambition to improve services through the greater use of personal information. Its Service Transformation Agreement[6] conveyed the same message. Announcing this review on 25 October 2007 in his speech on liberty[7], the Prime Minister set out the Government's belief that 'a great prize of the information age is that by sharing information across the public sector - responsibly, transparently but also swiftly - we can now deliver personalised services for millions of people'.

1.10 The tenor of the Government's argument has focused closely on the benefits of data sharing, paying perhaps too little attention to the potential hazards associated with ambitious programmes of data sharing. The Government has consequently laid itself open to the criticism that it considers 'data sharing' in itself an unconditional good, and that it will go to considerable lengths to encourage data-sharing programmes, while paying insufficient heed to the corresponding risks or to people's legitimate concerns. In its report on the protection of private data, the Justice Select Committee[8] said:

'There is a difficult balance to be struck between the undoubted advantages of wider exchange of information between Government Departments and the protection of personal data. The very real risks associated with greater sharing of personal data between Departments must be acknowledged in order for adequate safeguards to be put in place.'

1.11 Moreover, there has been growing concern – rightly or wrongly – that the Government's default position is to endorse the sharing of personal information for a given programme before considering whether it is in fact necessary to do so. In her submission to this review, Rosemary Jay, a legal expert in data protection, described the Government's Vision of data sharing as follows:

[2] http://www.cabinetoffice.gov.uk/strategy/work_areas/privacy/~/media/assets/www.cabinetoffice.gov.uk/strategy/piu%20data%20pdf.ashx
[3] http://www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf
[4] http://www2.cst.gov.uk/cst/reports/files/personal-information/report.pdf
[5] http://www.foi.gov.uk/sharing/information-sharing.pdf
[6] http://www.hm-treasury.gov.uk/media/B/9/pbr_csr07_service.pdf
[7] http://www.pm.gov.uk/output/Page13630.asp
[8] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf (paragraph 29)

'While I know this is an extreme (and rather unkind) analogy it is rather like wishing to encourage better nutrition among school children by having a "vision" of grating or peeling or some other culinary process rather than a vision of healthier children.'

1.12 During the course of our review, many people made comment about specific Government initiatives involving the wider use of personal information, including proposals for a national identity card and the related national identity register, and about ContactPoint. Our task however was not to look at specific projects but to review the general principles governing the use and sharing of personal information. For this reason, we make no recommendations about individual data-sharing schemes.

1.13 The Government and the private sector's apparent drive to collect, use and share more personal information is not the only concern. Recent high-profile data losses by both public and private sectors have drawn attention to the increased capabilities of technology, the risks of identity theft and the need to keep personal information safe from fraudsters. All this has pushed issues of data sharing and data protection significantly higher up the political agenda, even as our review has been in progress. Until recently, it was inconceivable to most people that just two CDs could store some 25 million records, containing financial details of people in receipt of child benefit. Their loss by HM Revenue & Customs[9], together with the loss of bank and insurance details by banks, building societies and other financial institutions[10] have served as stark illustrations of the risks posed by the 'information age'.

1.14 Anxieties over the risks and benefits of personal information sharing, and the impact it can have on people's privacy, spread far beyond the UK, and are currently the subject of serious debate in Europe and around the world. Indeed, the European Commission has recently announced that it is commissioning a study to review the adequacy of the Data Protection Directive[11].

1.15 However, the use and sharing of personal information are now permanent features of modern life, supported by mushrooming technological advances in the storage, analysis and use of large datasets. Public, private and voluntary-sector organisations will continue to require access to personal

[9] There have been a number of reports published recently by the Government in the aftermath of the HMRC data loss and other cases concerning the Ministry of Defence. The Poynter review (http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf) and the Independent Police Complaints Commission report (http://www.ipcc.gov.uk/final_hmrc_report_25062008.pdf) looked at the HMRC case. The Burton review (http://www.mod.uk/NR/rdonlyres/3E756D20-E762-4FC1-BAB0-08C68FDC2383/0/burton_review_rpt20080430.pdf) looked at the MOD cases. The Cabinet Secretary, Sir Gus O'Donnell also published a wider report (http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx) looking at data handling across government.

[10] See for example the Financial Services Authority report: *Data Security in Financial Services* (April 2008). http://www.fsa.gov.uk/pubs/other/data_security.pdf

[11] http://ted.europa.eu/Exec?DataFlow=ShowPage.dfl&Template=TED/N_one_result_detail_curr&docnumber=117940-2008&docId=117940-2008&StatLang=EN

information in order to provide goods and services, combat crime, maintain national security and protect the public.

Public perceptions and attitudes

1.16 Public interest in the security of personal information is not new, neither are concerns about the way organisations handle personal information. According to the recent European Commission longitudinal study, *Flash Eurobarometer*[12], public unease about the use of personal information is widespread and has remained consistent for almost twenty years. Some 64 per cent of EU respondents – and as many as 77 per cent of UK respondents – expressed concerns about whether organisations holding their personal data handle it appropriately. Almost exactly the same proportion of respondents identified similar concerns in Eurobarometer's 1991 survey, with little fluctuation in between.

1.17 On public trust issues, Eurobarometer's findings are especially interesting for the views they reveal about particular sectors. Medical services and doctors were trusted by 82 per cent of EU respondents, and the police by 80 per cent; for the UK those figures were 86 per cent and 79 per cent respectively. By contrast, mail order companies were trusted by just 24 per cent of EU respondents and travel companies by 32 per cent. In the UK, those figures were 26 per cent and 35 per cent respectively. Market and opinion research companies scored lowest among UK respondents, achieving a 25 per cent trust rating.

1.18 Over the last few years a large number of UK polls and surveys have tracked public attitudes to these issues, as well as the opinions of practitioners who process personal information, and of the organisations that employ them. The British Computer Society's *Data Guardianship Survey 2008*[13] found that around nine out of ten respondents felt that it was either very important or quite important that individuals should have an automatic right to correct data held on them where there were errors. Similar proportions believed that they should be able to find out who has access to their information and for what purpose; and that they should be asked for their consent if third-party organisations wanted to access personal information held about them. Reflecting recent stories about data breaches and losses, 66 per cent of respondents reported a decrease in their level of trust in established institutions (such as government departments) to manage their personal information correctly. In a similar vein, research published by the Information Commissioner's Office (ICO) in March 2008[14] illustrates the effects of recent data-loss scandals on public attitudes. Individuals are now more likely to check their bank statements regularly, for

[12] Eurobarometer: Data Protection in the European Union – Citizen's perceptions (February 2008). In total, 27,074 interviews were carried out across the EU, with 1,001 in the UK during 08 – 12 January 2008 - http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[13] BCS Data Guardianship Survey 2008 used a representative sample of 1,025 adults aged 16 and over. Interviews were carried out during 11 – 15 January 2008 - http://www.bcs.org/upload/pdf/dgs2008.pdf

[14] UK Consumers Wake Up to Privacy: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/icm_research_into_personal_information_feb08.pdf

example, and will refuse to share their personal information wherever possible, in an effort to prevent fraud.

1.19 Surveys have also sought the opinions of data-protection professionals and of large corporations. A survey by Privacy Laws & Business (April 2008)[15] found that more than four-fifths of data-protection professionals supported increased powers for the Information Commissioner to audit organisations in their sector, while 75 per cent would support the introduction of a new criminal penalty for major breaches of data security. According to Privacy Laws & Business, these findings reflect the fact that professionals want their organisations (and more particularly their superiors) to start treating data security more seriously, and they see a more robust regulatory regime as the way to achieve that goal. The Deloitte Technology, Media & Telecommunications survey (2007)[16], which took evidence from over 100 large global companies in the Technology, Media & Telecommunications sector, also suggested that large businesses must increase their security efforts and investments to avert security crises.

Conduct of the review

1.20 Once the review secretariat was established we issued a consultation paper on 17 December 2007, requesting responses by 15 February 2008. We received some 214 submissions in response from organisations and individuals with an interest or expertise in this topic, including local government, central government departments, financial and commercial institutions, legal professionals, healthcare providers, medical researchers and funders, industry, professional bodies, academics and civil society groups. The organisations and individuals who contributed to the review are listed in *Annex B*, and a summary of the submissions received is at *Annex C*.

1.21 We held seven facilitated discussion sessions in February, March and April 2008. Six of these were generalist workshops with participants from a range of organisations and institutions, and one was a dedicated legal workshop with participants from law firms and legal academics specialising in data protection and privacy matters. Notes of these meetings and a paper summarising the key themes are available at *Annex D*. Intellect, the trade association for the UK technology industry, organised a separate workshop in order for its members to feed in to the review. A note of that session is also included in the annex.

1.22 Between us and the secretariat, some 60 further meetings were held with a wide range of parties. Visits were also paid to the European Data Protection Supervisor and the Secretary of the European Commission's Article 29 Data Protection Working Party, and the devolved administrations in Scotland and Wales. The Office of the First Minister and Deputy First Minister of Northern

[15] http://www.privacylaws.com/Documents/PL&B_UK_SPL/uknews36.pdf
[16] http://www.deloitte.com/dtt/cda/doc/content/TMT%20Security%20Survey%20-%202007%282%29.pdf

Ireland participated in one of the discussion sessions and submitted a consultation response.

1.23 The secretariat further conducted an extensive literature review, a non-exhaustive bibliography of which is listed at *Annex E*.

1.24 The evidence informed the review's discussions, its conclusions and recommendations. We are grateful to all who responded to our consultation, participated in the workshops and were able to spare some of their valuable time to speak to us during the course of the review.

2. The scope of information sharing

2.1 It is impossible to generalise about the sharing of personal information. In itself, the sharing of personal information is neither good nor bad; in some circumstances sharing information may cause harm, while in others, harm may flow from not doing so. Whether or not to share information must be considered in context and on a case-by-case basis.

2.2 For anyone wishing to share personal information, the relevant questions are: What information do you wish to share? What is your purpose in sharing this information? Can you achieve your purpose without sharing the information? Are you confident that you are sharing no more and no less information than is necessary? Do you have the legal power to share the information? Do you have the technical competence to share information safely and securely? What safeguards will counter the risks that will necessarily arise as a result of sharing? By what means and on what basis did you or will you acquire the information? The answers to these questions provide the basis for designing and evaluating any proposal to share information.

2.3 A simple taxonomy of three basic types of data sharing has emerged from the many different examples of sharing considered during the course of this review. This covers:

- sharing for the purposes of law enforcement and public protection;
- sharing to provide or improve services in the public and private sectors; and
- sharing to facilitate statistical analysis and research.

2.4 In this chapter we briefly consider each of these types of data sharing and identify the major principles and issues that arise.

Law enforcement and public protection

2.5 Personal information must often be shared to protect national security, help prevent crime, and identify the perpetrators of crime. Agencies, typically but not necessarily in the public sector, are increasingly sharing or pooling relevant information about people identified as presenting the risk of harming others. Public protection covers policing, crime prevention and detection, national security, and protecting vulnerable people considered to be at risk of harm from themselves or from others.

2.6 It is self-evident that personal data must be shared in order to achieve these purposes, but this begs questions about the scale and circumstances of sharing. Even with the best intentioned motives, sharing cannot be contemplated on an unlimited basis.

2.7 During the last few years, there has been an enormous increase in the amount of personal information collected about the everyday lives and

activities of every citizen. This information may relate to people's characteristics; their behaviour and activities; and to their transactions. There can be considerable interplay and overlap between these categories.

2.8 There is no simple answer to the question of when it might be appropriate to share personal information for enforcement and protection purposes. In each case a proportionality test is the most appropriate consideration. A test of proportionality is a topic to which we will return throughout this report. We mean by this the application of objective judgement as to whether the benefits outweigh the risks, using what some might call the test of reasonableness or common sense. Proportionality involves making a considered and high-quality decision based on the circumstances of the case, including the consequence of not sharing. Decisions must flow especially from the principles of relevance and necessity and the need to avoid an excessive approach. This means asking such questions as:

- what benefits are sought from the proposed sharing?
- what harm will be curbed or prevented?
- how are the purposes articulated?
- what personal information is relevant?
- with whom will it be shared?
- what information is it necessary to share?
- can less information be shared or retained for shorter periods?
- what will be the likely effect on individuals and society?

2.9 For instance, following the terrorist attacks on the London Underground on 7 July 2005 there was little public concern about the extent of personal data sharing that ensued. Video recordings from surveillance cameras on national and London rail and underground networks were subsequently shown publicly, just as surveillance footage is routinely screened for the purposes of identifying the perpetrators of serious crimes. Similarly, information from mobile phones was used to establish the location and ultimate identification of the terrorists of the 2004 Madrid train bombings. Positive views of the use of surveillance film to catch the perpetrators of serious crimes are nonetheless challenged by public concern at the rapid increase of surveillance cameras in public spaces. But on issues revolving around the resolution of serious crimes, public concern tends to focus on the failures of data sharing rather than its excesses.

2.10 During this review, we came across many instances when sharing personal information had helped to detect and stop criminal activities. For example, by cross-matching the data it controlled with various databases operated by other agencies, the Serious Organised Crime Agency (SOCA) helped to uncover a significant fraud in the issuing of UK passports. The operation resulted in the prosecution and conviction of the perpetrator, and led to changes in the way risks are managed, thereby improving the security and integrity of the passport application procedure.

2.11 By contrast, the sharing of personal information is strongly contested in the enforcement of lesser offences. A recent example is the use of the Driver and Vehicle Licensing Agency (DVLA) database by private car-clamping companies for the civil enforcement of parking infringements. In similar vein, Poole Borough Council's use of surveillance techniques to establish whether a child was living in the catchment area of a local school has been widely criticised[17]. Both received adverse media coverage and, in the case of the DVLA database, provoked many letters of complaint to the Information Commissioner and even to the European Commission. During the course of our consultation we encountered people with equal and opposite views on the appropriateness of data sharing in each of these examples.

2.12 Similar issues of proportionality apply in the case of protection. A good example of multi-agency co-operation is the Multi-Agency Risk Assessment Conferences (MARACs) scheme, where statutory and voluntary agencies likely to come into contact with victims of domestic abuse share information and work together to compile as complete a picture as possible of the risks faced by victims and their children. Sharing this information enables multi-agency safety action plans to be developed to provide a coordinated response to reduce further victimisation and domestic abuse. MARACs currently operate in 100 areas, and data suggest that there has been an average reduction of 50 per cent in repeat victimisation in those cases reviewed at MARACs[18].

2.13 Disclosures made under Part V of the Police Act 1997 further illustrate how sharing information can help to prevent harm. In this case, information provided by the Criminal Records Bureau to certain categories of employer, typically those working with vulnerable groups, should help them to make well-informed judgments on the suitability of potential employees.

2.14 However, sharing personal information to protect the public can also raise controversial questions. For example, is it appropriate that the Government and utility companies share information about people's fuel bills in order to identify people who may find themselves in fuel poverty following the recent large rises in gas and electricity prices? The Government's plans have been welcomed by some, but condemned by others as excessive and intrusive, especially given the potentially stigmatising effects. And when is it appropriate for a doctor to breach fundamental principles of confidentiality in the doctor-patient relationship? More specifically, if a patient has the potential to harm others, in what circumstances can a medical practitioner share information? The point at which the line is drawn is inevitably a subjective one based on difficult ethical considerations and professional judgement. There are fears that a misunderstanding of data protection law

[17] In the light of the example of Poole Borough Council, and that of certain other local authorities reported to have acted in a similar way, we welcome the advice to local authorities from Sir Simon Milton, chair of the Local Government Association, urging councils not to use surveillance powers to police 'trivial offences'.

[18] See page 43 of Home Office Report: *Saving Lives. Reducing Harm. Protecting the public. An action plan for reducing violence 2008-11:* http://www.homeoffice.gov.uk/documents/violent-crime-action-plan-08/violent-crime-action-plan-180208?view=Binary.

can result in decisions being deferred and members of the public coming to harm as a result of a failure to share information.

Service delivery

2.15 In the public, private and voluntary sectors, providing services depends in many cases on sharing personal information. Here, people are primarily customers in search of a product or service – be it education or healthcare, life insurance, a flight, or an album download. Many object to the receipt of marketing materials, historically a major source of complaint to the Information Commissioner's Office. But we suggest that people are generally less concerned about (and possibly less aware of) the information flows that facilitate the provision of goods and services to them.

2.16 The provision and delivery of services nonetheless raise important questions about proportionality when the sharing of personal information is involved:

- is sharing personal information necessary for the provision of the service?
- is more information shared than the service requires?
- is the customer aware of the nature and extent of the sharing?
- what mechanisms are needed to alert citizens to services they are neither receiving nor seeking, but from which they might benefit?

Is sharing personal information necessary for the provision of the service?

2.17 Healthcare provides a clear example of the need to provide personal, and in many cases very sensitive, information in order to receive treatment or other services. Evidence submitted to the review illustrates that sharing personal health information can play a critical role in making sure that patients receive the safest, most effective and timely care possible. Efficient referrals from GPs to specialists in hospitals and from specialists to wider care teams are almost entirely non-contentious. They help ensure that patients' health problems are dealt with promptly and as effectively as possible. Care teams need to be aware of the patient's medical history so as to avoid incorrect diagnoses or repetitive testing. Moreover, in emergencies such as cardiac arrests or serious accidents, sharing information swiftly could prove vital to a patient's survival chances, as could the immediate notification of a suitable organ available for transplant. Furthermore, sharing personal health data for administrative purposes, and for auditing of clinical practices, safeguards public money, improves clinical care, is vital for planning purposes and helps to target resources to areas of greatest need, thereby reducing inequalities in service provision – the 'healthcare lottery'.

2.18 In order to be proportionate, it is often necessary to consider how much personal information, if any, is needed to carry out a particular transaction. An important and frequently overlooked distinction in the provision of services is between credentials and identity. In some cases it is unnecessary to exchange explicit personal information; it may be enough to present a credential proving a person's eligibility to receive a particular

service. A good example of this is an old person's bus-pass, which bears a picture and confirms eligibility, but which does not bear a name, or date of birth or even age. Another obvious example is the use of a PIN code authenticating a credit or debit card transaction. In the purchase of services, the service provider rarely needs to know anything about the identity of the purchaser, merely that the purchaser has the necessary credentials to make a payment.

Is more information shared than the service requires?

2.19 When buying goods and services, we frequently provide more information than is necessary to companies who seek to use or share our information for marketing purposes. Many people have joined retailers' loyalty or reward card schemes. These allow companies to analyse the purchases we make and to despatch marketing materials based on this analysis. This is part of modern commercial life, a matter of choice and attractive to many consumers. The relatively very small numbers of complaints that loyalty card operators and major retailers receive about this suggest that members understand it well enough and benefit from it. In some cases, groups of stores participate in combined reward cards, but we understand that they are zealous not to lose competitive advantage, nor to alienate their customers, by sharing detailed information about shopping habits among themselves.

2.20 The internet is being used increasingly to buy goods and access services. It is easy to overstate the difference between the online and 'bricks and mortar' commercial models. However, it seems that online retailers, in particular, process information about people's online activities much more intensively, and arguably more intrusively, than in traditional contexts. For example, it is possible for online retailers to suggest future purchases to customers based on their previous purchases, or to target advertisements based on previous website searches.

2.21 An extraordinary internet phenomenon of recent years is the development of new services based purely on the sharing of personal information. There are two examples of this. First, the web has enabled the development of social networking sites on which people place extensive personal information about themselves in order to share this information with a network of 'friends' or other groups selected and authorised by them. However, there is evidence that people who lack awareness of the consequences of extensive disclosure, or who are lax about restricting their social network to people they know, may disclose personal information to complete strangers, with all the attendant risks.

2.22 Another unique internet-born phenomenon is the advent of companies that operate by taking people's personal information from publicly available sources – such as the electoral register, company registers, phonebooks and websites – and aggregating these sources to form extensive personal data files. Customers, or more usually subscribers, are then charged to

access these files. The full implications of this sort of service have yet to be studied and we make a recommendation about this in Chapter 8.

Is the customer aware of the nature and extent of the sharing?

2.23 In some business sectors, organisations share extensive amounts of data. Banks and providers of credit, for instance, share detailed financial data at the level of individual transactions, mainly through credit reference agencies. The consumer benefits through easier access to financial services, lower costs flowing from better risk assessment, and lower levels of fraud, which may be identified by unusual patterns in financial transactions. The sharing is also justified in terms of promoting more responsible lending and borrowing. Although people are advised when credit checks are carried out, at least in the small print, it is far from clear whether enough people are aware of the extent to which information is shared in this way, or whether people consider it appropriate and proportionate to the risks.

2.24 Many instances of information sharing can make life easier, cheaper and less troublesome. A good example of this, and one which seems to enjoy wide support, is the sharing of information between motor insurance companies, VOSA (the MoT certification authority) and the DVLA. This allows people to renew vehicle tax discs swiftly and easily through the DVLA's website.

What mechanisms are needed to alert citizens to services they are neither receiving nor seeking, but from which they might benefit?

2.25 Either through choice or lack of awareness, many citizens do not receive the public-sector benefits and services to which they are entitled. This raises important questions. Should the public sector attempt to provide services to those who do not seek them? When does well-intentioned concern become intrusive state paternalism? These are real and difficult dilemmas, especially as some people may wish actively to reject particular benefits. For example, some people have been seriously offended by receiving an age-related free bus pass, after their health authority had passed on their dates of birth. But does offence to a few trump the gratitude of others for receiving the service? In similar vein, it would be dangerous to assume that all parents receiving income support would wish this information to be disclosed automatically or routinely to schools to secure free meals for their children. Likewise, some people may really suffer if fuel subsidies to alleviate fuel poverty are not readily available, while others may object strongly to their social security details being passed on to a utility company.

2.26 Identifying people entitled to services and benefits may be helped by the sharing of personal information across central and local government, and in some cases with the private sector, for example utility companies. But again the question of proportionality arises: which services are sufficiently important to people to merit the sharing of information about them? What information about their needs and eligibilities would people find excessively embarrassing, intrusive or stigmatising?

2.27 To conclude, organisations that can share information between themselves should be able to provide better, cheaper, faster and more personalised services to the public. A good example is illustrated in Box 1, below. As always, however, the questions that need to be considered in each situation revolve around proportionality, transparency, consent, accountability, and the careful design of the mechanics of any scheme, including a clear strategy for communication.

Box 1: Motor Insurers' Information Centre
A wholly owned subsidiary of the Motor Insurers' Bureau (MIB), the Motor Insurers' Information Centre (MIIC) was established initially to implement an industry-wide database of motor insurance information, providing a central source to assist in the fight against crime. Its Motor Insurance Database (MID), populated by information from private-sector insurance companies, is used by public sector organisations, particularly the police who are now the MID's biggest customer, making over 3.8 million enquiries per month. The DVLA, with over a million enquiry transactions each month in support of their Electronic Vehicle Licensing operation, is the second largest user of the MID. The links between MID and DVLA have facilitated the online car tax renewal scheme, which enables vehicle owners to avoid Post Office queues or the need to post their documentation, allowing them instead to pay their car tax from the comfort of their own home.

Research and statistics

2.28 Sharing personal information for the purposes of research and statistical work represents the third important category of sharing. This has produced benefits in almost all areas of life – whether in better designed roads resulting in fewer road traffic accidents; the removal of asbestos from buildings following the establishment of causal links between asbestos and mesothelioma; or early educational interventions to identify categories of young people at risk of under-achieving.

2.29 Concerned with populations rather than individuals, this type of sharing should theoretically pose fewer problems. Anonymised and statistical information is not subject to the DPA. But life is never simple, and even here, issues of consent, confidentiality and scope require attention.

2.30 Healthcare services illustrate many of the key issues discussed in this report. The training of doctors and other healthcare workers rightly emphasises the crucial importance of confidentiality. A belief in absolute confidentiality allows patients to tell their doctors their most intimate personal health secrets in return for treatment. But this confidentiality is in fact not so absolute. Treatment normally depends on sharing those personal secrets with other members of the health team. Doctors write letters to other health professionals, revealing the full details of a person's medical problem. Administrative staff open these letters before passing them on to the addressee. People hand over prescriptions that reveal sensitive diagnoses

to pharmacy staff in high-street chemists. We tolerate this sharing because we believe that all these individuals are bound by a duty of confidentiality, and we recognise that healthcare services require this extended health team. We also accept that the limits on sharing information within the health team can be breached if obvious public harm can be avoided as a result. For example, a doctor may pass the name of an alcoholic driver of a public service vehicle to the DVLA. The doctor will usually advise the driver to notify the DVLA personally, but should indicate that, even in the absence of the patient's agreement or even in the face of strong objection, the doctor will pass this information to the DVLA.

2.31 The foundation of modern medicine is research - into the prevention of disease, the nature of disease, and the health of individuals and populations. Such research depends on the study of individuals and populations. Much of this research is conducted in immediate partnership with patients who provide consent to that research, for example to participate in trials comparing different medicines in the treatment of a disease. Medical research in the UK is well governed and must be scrutinised and approved by a properly constituted research ethics committee. However, there are circumstances in which specific individual consent to participate in medical research is virtually impossible. Public health research involves large populations and has led to major gains in human health throughout the world. This research depends on the use of aggregated personal data.

2.32 Why does this pose a problem given that the identity of specific individuals within the populations under study is not relevant to the research, and no harm can flow to individuals as a result of the research? In order for research of this type to be conducted, personal information has to be accessed by someone in order to be aggregated and, even if names and addresses are removed from the final dataset, there remains the possibility that individuals could be identified from the coded dataset Box 2. However, consent is not feasible for such public health research because the whole population of the UK could not be approached individually to take part in database studies of public health. Would it matter if only a fraction of the population who did give specific consent participated in such studies? The answer is yes and an example that illustrates the harmful bias generated by selective participation is illustrated in Box 3 below.

Box 2: Power lines and risk of leukaemia
Researchers wish to study whether living near power lines is associated with an increased risk of leukaemia in children. In order to do this they need a complete regional or national registry of individuals with leukaemia, coupled with postcode information linked to the geography of power lines. At some stage in the processing of the database that can enable this study, it will contain information that a child of a particular age lives in a specific postcode. These two pieces of information alone could enable the specific identification of that child.

Box 3: Abortion and risk of breast cancer

Although it is now accepted that there is no increased risk of breast cancer associated with induced or spontaneous abortion, this important finding took a long time to establish. Indeed, a number of early studies suggested that there was such a link between abortion and breast cancer. Relying on respondents to recollect and report previous abortions, these early studies had looked at relatively small numbers of women, included them only after they had developed breast cancer - and women with breast cancer were more likely to report a previous history of abortion than healthy women without breast cancer.

By contrast, much larger studies gathering data from women before they developed breast cancer and from medical records have shown no association between spontaneous or induced abortion and the incidence of breast cancer.

The benefits for public health of undertaking this type of research are clear. This example also illustrates why it is important to study large unselected populations in an unbiased fashion.

3. The legal landscape

3.1 Sharing data across and between organisations can be a complex process. As there is no single source of law regulating the collection, use and sharing of personal information, these activities are governed by a range of express and implied statutory provisions and common-law rules. Yet despite, or more likely because of, this broad range of provisions, the legal basis setting out whether and how information can be shared in any given situation is often far from clear-cut.

3.2 For practitioners dealing with everyday questions about whether or not to share information, the picture is often confused. The absence of clear legal advice either specifically sanctioning or preventing information sharing typically results in one of two outcomes. People either make decisions based on what feels right to them as professionals, albeit with concerns that their approach may not accord exactly with the law. Or (and perhaps the greater temptation for many) they defer decisions altogether, for fear of making a mistake.

3.3 Below we set out the key components of the legal framework, which illustrates the complexity that practitioners face.

The European Directive

3.4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[19] (widely known as the 'Data Protection Directive') concerns the protection of individuals with regard to the processing and movement of personal data. It is a harmonising measure, which binds Member States who have an obligation to transpose it into domestic law. Breaches of the Directive can be challenged by the European Commission and are reviewable by the European Court of Justice.

3.5 The original objectives of the Directive focused broadly on protecting the right to privacy in the processing of personal data, while ensuring the free movement of such data within the European Union. Fuelled in part by technological, commercial and social developments since its adoption in 1995, voices in some quarters are increasingly questioning whether the Directive, and by inference the UK's Data Protection Act, is still fit for purpose. Some are calling for the Directive to be reviewed. The UK's Information Commissioner has recently awarded a contract to RAND Europe to conduct a review of EU data protection law[20]. The European Commission itself is also now seeking tenders to conduct a comparative study on different approaches to new privacy challenges in the light of technological developments. The Commission's aim is to 'give guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered in the light of best solutions identified'.

[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
[20] http://www.ico.gov.uk/upload/documents/pressreleases/2008/invitation_to_tender_1404081.pdf

3.6 While evidence to this review criticised aspects of the Directive, the point was generally accepted that there is very limited scope for, or value in, a fundamental review of UK data protection law in isolation. Analysis of the Directive goes beyond our remit, but we are pleased that the recent reviews are now under way. Although neither constitutes an official EC review of the Directive, any changes to the EU Directive will eventually require changes to UK's Data Protection Act. This may still be some years away, however, and the recommendations of this review are set in a UK context and are directed at a more immediate agenda.

3.7 However, it is extremely important that the UK Government engages actively in review and reform of the EU Directive. We therefore recommend in this report that the Government should participate actively and constructively in the current European reviews and lead Member State and wider debate about reform. This will shake off any impression that successive governments have been lukewarm about data protection. More importantly, as data flows become ever more global, the Government has the opportunity to demonstrate its leadership by bringing forward practical international approaches to data protection, rather than simply responding to the proposals of others.

The Data Protection Act

3.8 The main piece of UK legislation governing data sharing is the Data Protection Act 1998[21] (DPA). Replacing the Data Protection Act 1984, the DPA primarily transposes EC Directive 95/46/EC into UK law and regulates the collection, use, distribution, retention and destruction of personal data. Personal data are defined in Part 1 of the Act, but they broadly mean any data relating to a living individual who can be identified from those data. The DPA is built around the Directive's principles of good practice for the handling of personal information, some of which are particularly relevant in the context of information sharing. For example, the principles require that any processing of personal information is necessary, and that any information processed is relevant, not excessive and securely kept. Processing is a wide concept covering collection, use and sharing. The principles are intended to provide a technology-neutral framework for balancing an organisation's need to make the best use of the personal details it holds while safeguarding that information and respecting individuals' private lives.

3.9 The DPA also establishes various rights for individuals (inappropriately described as 'data subjects'), notably a right of access to information about themselves. It also requires almost all data controllers to notify a general description of their data-processing activities to the Information Commissioner, the independent statutory officer responsible to Parliament for regulating the DPA. The Commissioner has various functions – discharged through his office (ICO) - aimed at promoting good practice, providing guidance, resolving complaints and enforcing the law.

[21] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Human Rights Act

3.10 The Human Rights Act 1998[22] gave full effect in UK law to the rights contained in the European Convention on Human Rights (ECHR). It is unlawful for a public body to act in a way that is incompatible with ECHR rights (section 6).

3.11 Article 8 of the ECHR is particularly important when considering data sharing and privacy matters. This provides that a person has the right to respect for his or her private and family life, home and correspondence. A public body wishing to interfere with this right will need to prove that it is acting lawfully, and that its actions are in the pursuit of a legitimate aim that is necessary in a democratic society. To satisfy human rights requirements, compliance with the DPA and the common law of confidentiality is necessary, but not always sufficient by itself.

Common law

3.12 The power to collect, use, share or otherwise process information can be derived from common law, as can restrictions on these powers, such as the common-law duty of confidentiality. A breach of confidence can occur when information that one might expect to be confidential is communicated in circumstances entailing an obligation of confidence, but later used in an unauthorised way. Contractual agreements can also provide the basis for collecting, using and sharing personal information, and organisations and individual practitioners should also take into account any relevant professional guidance or industry code.

3.13 Government departments headed by a Minister of the Crown may be able to rely on common-law powers to share data where there is no express or implied statutory power to do so. The general position is that the Crown has ordinary common-law powers to do whatever a natural person may do (unless this power has been taken away by statute).

3.14 In addition to common-law powers, the Crown also has prerogative powers. Although there is no single accepted definition of the prerogative, these powers are often seen as the residual powers of the Crown, allowing the executive to exercise the historic powers of the Crown that are not specifically covered by statute. Residual powers may relate to foreign affairs, defence and mercy, for example. However, Parliament can override and replace prerogative powers with statutory provisions.

3.15 Public bodies which are established by statute (e.g. local authorities and HMRC) have only such powers as are conferred upon them by statute. This means that those bodies have no powers under the common law or the Crown prerogative and must rely solely on their express or implied statutory powers.

[22] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1

Administrative law

3.16 Administrative - or public - law is the body of law governing the activities of government and other public bodies. Before a public body can engage in data sharing, it must first establish whether it has a legal power to share the data in question. Where a public body acts outside its powers, the activities can be challenged before the courts by way of a judicial review.

3.17 The nature of the public body and the rules governing its activities play a crucial part in determining the legal basis upon which it acts and whether its activities are lawful. If a public body does not have the power to collect, use, share or otherwise process data, it will be acting unlawfully; and the fact that an individual may have consented will not make the activity lawful.

Statutory powers

3.18 Non-ministerial departments or those created by statute cannot have prerogative or common law powers. Any data sharing by them must be based on statutory powers (express or implied), while statutory powers can also impose obligations on non-public bodies to share or disclose information. For example, section 52 of the Drug Trafficking Act 1994 makes it an offence to fail to report suspicion of drug money-laundering activities, thereby placing a statutory duty on people and organisations to share relevant personal information with the police.

Express statutory powers

3.19 Express statutory powers can be enacted to allow the disclosure of data for particular purposes. Such powers may be permissive or mandatory. A permissive statutory power describes legislation that gives an organisation the power to share data, for example, Section 115 of the Crime and Disorder Act 1998. A mandatory statutory power requires an organisation to share data when requested. An example of this is Section 17 of the Criminal Appeals Act 1995.

Implied statutory powers

3.20 Even where there is no express statutory power to share data, it may still be possible to imply such a power. To this end, where the actions or decisions of a public body are incidental to meeting the requirements of an expressed power or obligation, they can be considered to have an implied right or power to act.

3.21 Statutory bodies carry out many activities on the basis of implied statutory powers. This is particularly true of activities such as data collection and sharing, which are not always express statutory functions.

3.22 In order to imply a power to share data, the body in question must first of all be satisfied that it has the legal authority to carry out the core function to

which the sharing of data applies. Without the power to undertake the activity, there can be no implicit power to share data.

3.23 A public body sharing data under an implied power must also take account of any relevant conflicting statutory provisions that may prohibit the proposed sharing (either expressly or implicitly). Similar considerations should also apply to the collection of data. A body should consider whether collecting the data is reasonably incidental to existing statutory powers: i.e. whether it is fair to accept that this activity is reasonably associated with their existing powers.

Statutory bars

3.24 Legislation may also prohibit the disclosure of information or restrict disclosure to limited and defined circumstances. Section 18 of the Commissioners for Revenue and Customs Act 2005, for example, created a strict statutory duty for HMRC officials to maintain taxpayer confidentiality; and section 19 made any contravention of these provisions by such officials a criminal offence.

4. Key themes: Public trust and confidence

4.1 During the course of this review we gathered a wealth of evidence and opinion about the handling and sharing of personal information. On some issues we met with near-unanimous agreement, while on others we encountered a great divergence of views and even vehement disagreements relating both to the analysis of the problem and to the proposed solutions.

4.2 Irrespective of their divergent views, contributors repeatedly raised many of the same issues. These must be addressed if we are to resolve difficult questions about sharing personal information. The response to our consultation fell broadly into two main but inter-related areas. The first raised questions about the 'whether' of information sharing. These relate to the circumstances in which, and the extent to which, it is proper to share information; and to the mechanisms for deciding whether and what information should be shared. As might be expected, we encountered a significant divergence of views in this area, which we explore in the next chapter. The second group of responses focused on the 'how' of information sharing, covering a range of issues relating to good governance and technical competence. Here we encountered a wide measure of agreement about the major issues and their possible solutions. We explore this in Chapter 6.

4.3 First, however, we raise what was perhaps the most commonly recurring concern we encountered throughout the review: the low level of public trust and confidence in organisations' ability to handle and share personal information properly. In this brief chapter we consider the importance of public trust and confidence, drawing on the evidence submitted during the review and looking at differences in public attitudes towards information handling in the public and private sectors.

4.4 Public confidence in organisations' ability to handle personal information is at a low ebb. Opinion surveys over a long period have shown that people put little trust in the way organisations use their personal information. Recent high-profile and serious data losses by both public and private sectors have reinforced the commonly held belief that organisations do not look after personal information properly.

4.5 Evidence suggests that many people perceive problems in the public and private sectors differently. Attitudes towards the use of personal information are strongly coloured by the degree to which people feel they have choice and are in control of what information is collected about themselves, and how it is used. Public bodies frequently collect a wide range of information, often on a mandatory basis and sometimes without the knowledge of the individuals concerned. The personal information people disclose to public bodies may also be extremely sensitive: financial information for taxation purposes, health information for healthcare purposes, and a variety of other sensitive personal information from people applying for benefits. People are obliged to give public bodies personal information when registering births,

deaths and marriages, when applying for passports or paying for television licences, or when applying for school places for children. In the case of criminal or national security investigations, substantial volumes of personal information can be shared without people's knowledge. In all these situations, people have very limited awareness and control – or no control at all - over the information that is collected about them.

4.6 Given that the consequences of mismanaging such sensitive information can be serious and far-reaching, people have a clear and justifiable right to expect that these bodies will uphold the highest possible standards when handling and sharing their personal information. Where people are required by law to provide information to public sector bodies they can be particularly critical and unforgiving if the information is mishandled of misused. The risks of incompetent or excessive data handling can impact on society as a whole, far beyond the individuals directly concerned. The Orwellian spectre of 'Big Brother' is never far from the public mind when public bodies set out to collect, store and use personal data.

4.7 People also expect the private sector to maintain the highest standards when handling personal information. The misuse or mishandling of information by private-sector companies can have a very detrimental effect on individuals' lives, for example when they are the victims of identity fraud due to a bank's lax security, or when their fuel supply, telephone or internet access is turned off because of inaccurate payment records.

4.8 Banks, insurers, utility and telephone companies often have very similar terms and conditions for the collection and sharing of personal information. All these organisations wield considerable market power and people cannot easily function without them. Although a customer may choose one bank in preference to another or one phone company in preference to another, each company requires very similar personal information to others in its sector, and each shares significant amounts of information with credit reference agencies and other organisations. So within these sectors, individual choice and control over the collection and sharing of information are in reality also very limited, and we need to be confident that we can rely on these organisations to handle personal information appropriately.

4.9 Sharing personal information in both the public and private sectors means that information must cross boundaries, sometimes within organisations and sometimes between them. This includes cases that might not look like traditional data sharing, for example when information is sent to an external organisation for the purposes of backing it up. The sharing of personal information sometimes also means that it will pass across national boundaries.

4.10 All forms of sharing generate new risks. If public trust and confidence are to be ensured, these risks will need to be addressed. This is not just ensuring that security mechanisms are in place to protect information sufficiently well while it is being shared. It is fundamental that there is clarity about who is

responsible and accountable for all aspects of proper information handling at each of the various stages throughout the process of sharing.

4.11 In summary, the poor level of public trust and confidence in the sharing of personal information provides a critical backdrop to this review of data sharing. The next two chapters examine what this means in practice and highlight the need for substantial improvements in the ways that organisations handle personal information.

5. Key themes: Whether to share personal information

5.1 Consultation about whether information should be shared, and (if so) in what circumstances, raised some of the most contentious issues in this review. In our view, these form the most important part of our work. The core issues are:

- proportionality;
- consent;
- legal ambiguity;
- guidance; and
- people and training.

Proportionality

5.2 Proportionality, as defined in paragraph 2.8, lies at the heart of the discussion on data sharing. When considering whether personal information may or may not be shared, practitioners need to take a range of factors into consideration. Aside from questions of law, accountability and transparency, proportionality plays an important role in deciding whether it is appropriate to share information with others.

5.3 The question of proportionality is hotly contested in many areas where personal information is shared. For example, is the collection of personal information about every child in the ContactPoint children's database a proportionate way of balancing the opportunities to prevent harm and promote welfare against the implications for family privacy and the risks of misuse? Similarly, is a centralised collection of comprehensive health records in the National Health Service's Connecting for Health programme proportionate in balancing the opportunities to improve health care against cost and other considerations, including the risks to privacy if the system is abused, and the use of less 'joined-up' means of storing clinical information? What is proportionate in order to prevent fraud or serious crime? What is proportionate in order to counter a relatively trivial offence, such as dropping litter?

5.4 Many people worried by some of the large data-sharing schemes fear the likelihood of 'function creep', suspecting the first steps down a slippery path towards ever-greater use of personal information by an increasingly overbearing state. For example, a data-collection scheme that starts out with the simple aim of knowing that every child of school age is indeed in education could metamorphose into a system that maintains long-term records of each child's attendance, behaviour, exam results and physical or mental health. This in turn might be accessible to – and might influence – potential employers or law enforcement agencies decades later.

5.5 How should decisions about proportionality be made? One mechanism that could enable better decision-making is to conduct a privacy impact assessment to make clear the thinking behind a proposed data-sharing scheme and to demonstrate how the questions of proportionality are being

addressed. Privacy impact assessments are structured assessments of a project's potential impact on privacy, carried out at any early stage[23]. They enable organisations to anticipate and address the likely impacts of new initiatives, foresee problems and negotiate solutions. A second way to address issues of proportionality is to ensure data-sharing schemes are highly transparent and exposed to full public scrutiny. This would force those proposing the schemes to think through proportionality questions and defend them in public.

5.6 Respondents taking part in the consultation agreed almost unanimously that proportionality is the key to making sensible, defensible decisions about information sharing. It became clear, however, that we could not make recommendations that would give cast-iron answers to each and every question of whether to share personal information, now or in the future. The consensus was that a clear code of practice is needed to help organisations translate the concept of proportionality into a set of practical mechanisms for considering whether to share data, coupled with enhanced transparency for any information-sharing arrangement.

Consent

5.7 A prominent and recurring theme throughout the review was the degree to which people should be able to exercise choice and control over information about themselves. The debate over consent was polarised and complex, and no consensus emerged. This is not surprising.

5.8 We support the instinctive view that wherever possible, people should give consent to the use or sharing of their personal information, allowing them to exercise maximum autonomy and personal responsibility. However, achieving this in practice is not so simple. It is unrealistic to expect individuals ever to be able to exercise full control over the access to, or the use of, information about them. This is because of a number of factors, not least practical difficulties in seeking and obtaining consent in many circumstances. Moreover, there are many circumstances in which it is not useful, meaningful or appropriate to rely on consent, or indeed to obtain fresh consent at a later stage for the reuse of personal information for a different purpose.

5.9 A few practical questions illustrate the problem well: can consent ever be meaningful in contexts like law enforcement or taxation? Can people expect to receive a service but prevent the keeping of records about their use of it? Should organisations set up parallel systems because a minority refuses to join a system used by the majority? What happens when consent is withdrawn by an individual? Can patients expect medical treatment if they do not consent to information being shared within a healthcare team? Or as the Academy of Medical Sciences put it:

[23] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html

'The treatment of individual patients relies on data collected from others. This is challenged if a patient says "use my data to treat me, but not to improve care for others". Or more starkly, "use evidence from other people's data to treat me, but don't use my data to help them".'

Consent in different contexts

5.10 As set out in Chapter 2, we have identified three broad fields of data-sharing activity: public protection and law enforcement; service provision; and research and statistics. Issues around consent are different in each of these fields. For example, in the field of public protection, if a school were required to get consent to a criminal records check from a convicted sex offender applying for a job, vulnerable people could be put at risk. The public interest demands that such information is disclosed to potential employers, irrespective of the wishes of the individual. Furthermore, there are strong arguments that for research and statistical purposes, where the identity of individuals is not material to the research, a requirement to obtain consent could prevent or impede worthwhile studies and so damage the development of healthcare provision, for example. In this area, relying on individual consent to share data does not seem to be appropriate.

'Some forms of research, particularly those concerned with rare or long-term outcomes, such as side-effects of drugs or the incidence of rare cancers, or with environmental hazards whose effect is small at the individual level but significant across a large population, would be impossible or prohibitively expensive unless large datasets with complete, or near-complete population coverage are available. Such datasets are typically derived from routine sources, such as cancer and vital events registers. Their creation and use in research therefore entails sharing of personal information. Obtaining consent from every potential member of a large, population dataset would be an expensive but only partially successful undertaking. Willingness to take part in research is known to be socially patterned, so that if consent were required, coverage would be both incomplete and biased. On the other hand, the risk of harm to an individual from the inclusion of their records in such a dataset is minimal or zero. In cases like this, the requirement to obtain consent should take account of the balance of risk, cost and benefit.'

Medical Research Council

5.11 Consent is, however, more relevant in the provision of services, and where genuine choices can be made. Where the collection of personal information by an organisation is incidental to its core business, or where the effect of the data sharing could be achieved by other means, then it is only right that individuals should have the opportunity to decide how their information is used. For example, UK passport holders wanting to apply for a new photo-card driving licence can choose to send a new photograph with their application form to the Driver and Vehicle Licensing Authority, or they can consent to the DVLA obtaining their photographic image from the Identity and Passport Service (who will already hold the record). Some driving-licence applicants will want to take advantage of the streamlined service,

while others may have concerns about information security and so be unwilling to consent to it. In these circumstances, it is right that the individual should be able to decide.

5.12 There are many instances in which consent is the right mechanism for enhancing personal autonomy and its usefulness in these circumstances should not be underestimated, In such instances, however, we believe that organisations need to do more to make the request for consent transparent and easily understandable so that that when someone gives consent, the decision to do so is fully informed.

5.13 Nevertheless, we believe that it would be wrong to focus too heavily on consent as a means of legitimising information sharing. Indeed, European and domestic laws provide several alternatives to consent as the means of legitimising the processing of personal data.

False consent

5.14 In a case where consent is appropriate, the focus shifts to considering how consent should be handled. To have any meaning, consent must be free, genuine and informed. All too often, however, consumers are faced with standard terms and conditions that purport to seek their consent to process personal information in a particular way, but in fact offer no realistic choice at all. If someone applies for a credit card or a loan, for example, or if they want to access a computer software package they have downloaded or purchased, they will usually be asked to agree to a lengthy and technical list of specified terms, which include conditions relating to information management. Although these may be written and presented as securing consent, it will not feel like that to the consumer whose refusal to consent would automatically bar access to the product or service. Choice in such cases is limited and consent is false. Likewise, people are often asked for their consent on the basis of very little explanation, so they are unlikely to be able to make an informed decision about whether or not to give it.

5.15 Further, consent as a notion is too often devalued when it is requested irrespective of the data controller's ability or intention to abide by the response. For example, in some cases it will be necessary to collect personal information for audit purposes – and failure to collect it would mean that safeguards designed to protect people would simply fail. In such circumstances, seeking consent is meaningless and organisations should simply explain to people from the outset that their data will be used for specified purposes, clearly indicating both the reasons for this and the specific safeguards.

> 'As executor of my father's will I recently had to sign a "data protection consent" in order to close his Post Office account and receive the funds it held. When I asked why I had to sign, the answer was that my details were required by law and would be processed in the USA. If the gathering of data is strictly necessary, and I can see that in this instance it was needed for audit purposes, the data controller should not need the data subject's consent. Too many instances of consent bring the temptation to ask for consent for unnecessary purposes'
>
> **Respondent to the consultation exercise**

Fresh consent

5.16 'Fresh consent' – or 're-consent' – covers cases when people are asked to give consent again to the further use of personal information that was originally collected for a different purpose.

5.17 As a general rule, it seems right that personal information obtained consensually for a specified purpose should not then be used for an incompatible purpose that goes outside the terms of the original consent. If that were to happen, it would breach the terms of the original consent. For this reason, the second Data Protection Principle, which prohibits reuse of information in any manner that is incompatible with the original purpose, stands as a significant safeguard. It is important to note, however, that 'incompatible with' is not the same as 'different from'. Although some respondents to the review have said that the law should prohibit any reuse of personal information without fresh consent, we believe that returning to people on each occasion when an organisation wishes to reuse personal information for clearly beneficial and not incompatible purposes would impose a disproportionately heavy burden, particularly where the data pool is large.

5.18 Again, the example of medical research is particularly helpful here. Respondents in this sector agreed almost unanimously that a requirement to seek fresh consent for any supplementary use of previously collected personal information would be unworkable and have a severely detrimental effect on the ability to conduct important medical research. The time, money and effort required to do this would all have an adverse impact on research programmes and on patient care. This is an example where the principle of implied consent[24] is valid. An NHS patient agreeing to a course of treatment should also be taken to have agreed that information given during the course of the treatment might be made available for future medical research projects, so long as robust systems are in place to protect personal information and privacy. After all, that patient may be benefiting from research using health information from earlier patients.

[24] Implied consent is where consent flows from an initial decision to take up a service. For example, an elderly person receiving state-funded domestic assistance consents by implication that their eligibility will be checked and records will be kept of their use of service.

5.19 However, implied consent is not satisfactory without considerable transparency. In the case of the NHS, we strongly encourage it to build on its existing efforts to educate patients by making general and widely advertised statements about how people's health information might be used in the future[25].

5.20 We are of the view, therefore, that, in many cases seeking re-consent is not an appropriate or useful device. There are, however, lessons for researchers and others who seek to rely on individuals' original consent to legitimise further use of their personal information. Consent clauses should be written in a way that provides for reasonable additional uses of information, while giving patients and others sufficiently specific explanations and safeguards to prevent inappropriate uses or sharing of information about them.

Legal ambiguity

5.21 Responses to our consultation overwhelmingly pointed to a fog of ambiguity and uncertainty surrounding the legal framework to sharing personal information[26]. This is a particular issue at the interface between the public and the private sector, and we were given a number of relevant examples by consultees.

'The police are required to attend road collisions where a person has been killed or injured, the road is obstructed, or there are allegations of offences. The attending police officer will record information about the collision – including driver, vehicle and victim details, the circumstances of the collision, and the contact details of any witnesses.

Police road traffic collision (RTC) reports are a vital tool in helping motor insurers reach a decision where liability is in doubt, and therefore play a crucial role in resolving difficult claims as quickly as possible. Insurers want to pay timely compensation to claimants; this is in line with the Ministry of Justice's own commitment to making the personal injury claims process more efficient and cost effective to the benefit of claimants.

In the past, RTC reports were made available to insurers at a standard price, dispatched fairly promptly, and generally contained all the required material. Unfortunately, that is no longer the case. Today, vital information is often redacted. Data protection and human rights concerns are behind police refusals to supply full information. These concerns are we believe misplaced and should not override the broader interest of promoting access to justice'.

Association of British Insurers

5.22 When the case of Naomi Campbell v Mirror Group Newspapers reached the Court of Appeal, Lord Phillips (then Master of the Rolls) noted that the High

[25] This would help build on the commitment given by the Secretary of State for Health, the Rt Hon Alan Johnson MP, on 24 June 2008 about increasing involvement and choice for patients. See: http://www.dh.gov.uk/en/News/Recentstories/DH_085693.

[26] During the course of the review, the Information Commissioner's Office submitted various proposals aimed at revising certain provisions of the Data Protection Act. Some of the proposals range more widely than a focus purely on *sharing* data. However we publish the evidence in *Annex F*.

Court judge had described the path to his conclusion that Miss Campbell was entitled to compensation under the Data Protection Act 'as weaving his way through a thicket'. Lord Phillips went on to observe that 'the Act is… a cumbersome and inelegant piece of legislation'[27].

5.23 The problem does not seem to lie with the DPA's data protection principles. These are in themselves sound, balancing individual protection against the wider need to process and share information. They provide a sensible approach to handling and processing data, neither inhibiting nor promoting data sharing. However, our consultation has indicated unequivocally that the Data Protection Act does not, and maybe by itself cannot, provide a sufficiently practical framework for making decisions about whether and how to share personal data.

> 'The Act is a complex piece of legislation, but [one] which in practice boils down to some simple concepts of protection of data. However, this simpler view is almost never seen by the public or by organisations who struggle with the various concepts which provide (by necessity) many grey areas and few hard and fast rules.'
>
> **Data Protection Forum**

5.24 The Act's necessary breadth and openness are open to misinterpretation, or rather, they allow too much scope to interpret the Act in different ways, while even the name of the Act gives the misleading impression that organisations should seek to protect information from use by other organisations or for any additional purposes. Consequently, the Act is frequently interpreted too restrictively or over-cautiously due to unfamiliarity, misunderstanding, lack of knowledge or uncertainty about its provisions. As The National Archives said in evidence to us, 'There are many myths surrounding the DPA - it appears to be one of the most frequently cited yet least understood pieces of legislation.'

5.25 Although, on the face of it, the principles are fairly straightforward and easy to understand, the language of the DPA can be confusing and complex. Responses to the consultation singled out for special criticism the 'Conditions for Processing' (Schedules 2 and 3). Another area of concern related to the meaning of *personal data*, which while at first glance should prove to be a relatively simply concept, is in fact anything but. Indeed, the Act's definition in section 1 has given rise to considerable confusion and concern – and even to litigation, the results of which have done little to allay concerns. Box 4 illustrates the some of the problems currently posed.

[27] [2002] EWCA Civ No: 1373, paragraph 72. See: http://www.hmcourts-service.gov.uk/judgmentsfiles/j1364/Campbell_v_MGN.htm

Box 4: Defining Personal Information

Everybody seems clear that records kept by reference to traditional identifiers, such as a person's name and address, are caught by the DPA. However, the situation is far less clear in respect of information such as internet IP addresses or CCTV footage. Information like this could be combined with other information to allow an internet user or person in a piece of CCTV footage to be explicitly identified, but might not in itself constitute 'personal data'. Organisations seem unclear as to how to treat 'potential personal data' like this. There are two possible courses of action. First, take the view that 'potential personal data' is not caught by the DPA and that none of the Act's rights or protections apply to it. Or second, assume that it is covered by the DPA and attempt to treat it like 'ordinary' personal data.

Either approach causes problems. In the first, the information is completely unprotected from loss or misuse because none of the data protection principles apply to it. In the second, it may be possible to keep the information secure or to be transparent about its collection, for example, but other provisions of the DPA cannot be applied to it in practice, for example the right of subject access or the Act's consent provisions.

As it stands, data protection is an all or nothing piece of law: either information is personal data and the whole of the legislation applies to it, or it isn't and none of it does. An obvious solution to this problem, but one which neither the DPA or the European Data Protection Directive seem to allow, is to apply some of the rules of data protection to 'potential personal data', but not all of them. In the medium and long term, we would encourage the development of data protection law that can be applied much more flexibly and in particular would press for germane revisions to the Directive, to allow subsequent change to domestic law. However, for practical purposes, the concept of 'protected personal data' set out by Sir Gus O'Donnell in his Data Handling Review is attractive. This is defined as any material that links an identifiable individual with information, which if released would put them at significant risk of harm or distress; or that relates to 1000 or more individuals not in the public domain. Sir Gus has determined that such protected personal data should attract particular technical protection inside government departments and agencies.

5.26 We recognise that the Information Commissioner's Office has devoted considerable efforts in recent years to providing and publishing practical guidance; nevertheless a great deal of inconsistency and confusion remains in its practical application. The DPA is still commonly cited as a reason not to release information when it may be perfectly legitimate to do so.

5.27 In addition to attempting to interpret the Data Protection Act, those who must decide whether it is legal to share information must operate within a wider but equally murky legislative framework.

> 'It is frustrating working in a Children's Service authority that you need to share information yet the supporting statute does not explicitly permit this. For example, the Children Act 2004 (section 10) lays down the duty to cooperate and it has to be assumed that this covers information sharing; however this section could have made specific provision for information sharing. Under current arrangements it is far from certain whether the sharing of sensitive personal data (without consent) about a child is permissible.'
>
> **Education Leeds**

5.28 Evidence submitted to the review suggests that the complicated patchwork of statutory and common law leaves people uncertain whether they are able to share personal information or not. Since much legislation governing personal information is confusing, and this lack of clarity surrounds the definition of personal data itself, it can be difficult for practitioners to understand which legislation plays the trump card.

5.29 This is particularly true in the public sector, where Government has compounded the problem by legislating through any uncertainty, creating large numbers of specific legal gateways for sharing personal information. In doing so, it has created the impression for some that the absence of a gateway means no power to share. The complex interaction and overlap between these legal gateways also causes considerable confusion. The existence or absence of a statutory gateway often distracts decision-makers from making a determination about whether it is right to share information in the particular circumstances of each case. However, the latter is the more important matter and so should command central focus.

> 'Overall the DPA works well, [but] the issues are more in respect of other legislation that has been created to complement and enhance information sharing – for example, S[ection] 115 Crime and Disorder Act, Freedom of Information Act, Human Rights Act, Children's Act, Housing Act. There is little clarity as to how this other legislation works with the DPA in terms of enabling information sharing, and under what circumstances each of these powers should be used.'
>
> **Association of Chief Police Officers**

5.30 Many respondents to the review felt that while the Data Protection Act itself may not be in need of radical overhaul, inconsistent interpretation of the Act and surrounding areas of law is particularly damaging. For these respondents, introducing clarity into the requirements and language of the Data Protection Act would help to lift the fog surrounding information-sharing activities, as would a better explanation of the interplay between common law, the Data Protection Act the Human Rights Act and the wider legal framework. To hasten this process, the message that came across most

strongly was the need for a clearer framework: one that demonstrates more clearly how proportionality should be the basis for sharing information for positive, beneficial purposes.

Guidance

5.31 Much guidance exists for anyone using personal information - some of it good, some less so. Another clear message emerging from the review is that guidance can be very helpful, but that too much of it currently causes confusion. As a result, 'most frontline staff hardly read, and in particular cases often do not follow … the volumes of manuals that descend on them to guide many aspects of their work'. [28]

5.32 Much of the available guidance focuses heavily on compliance with the Data Protection Act and the mechanics of sharing. While this may be useful, there is scope for more risk- and scenario-based guidance to help people decide whether sharing personal information is correct in a given situation – not simply from a strict legal perspective but also taking into account issues of proportionality in sharing information.

5.33 According to several respondents, the Information Commissioner's Office's Framework Code of Practice for Sharing Personal Information (reproduced in *Annex G*) and Privacy Impact Assessment Handbook[29] provide useful guidance; and the code of practice goes some way towards clarifying the main issues faced by decision-makers. We urge all organisations to regard the Information Commissioner's Office as the central source of clear, authoritative and widely focused guidance on information sharing, tailoring that guidance as far as possible to their own particular needs. In Chapter 8 we propose how the ICO's existing code could provide the starting point for a more authoritative statutory code.

People and Training

5.34 Many respondents to the review commented that processes, technologies and practices are only as good as the people using them, and that most data breaches and improper uses of personal information result from human error. Even with good guidance materials, confusion, uncertainty or ignorance within an organisation can easily arise if communication and training are not taken seriously. Top management needs to put in place good practices for collecting, using and (where appropriate) sharing information. These must also be communicated to the right staff, backed with suitable training programmes. Incubating the right approach in daily work routines requires constant effort, supported wherever necessary by rigorous control systems and disciplinary measures. All staff handling personal information must be made fully aware of its value, and of the increased risks that arise when it is shared outside the organisation.

[28] *The Glass Consumer*, Susanne Lace et al, Policy Press 2005
[29] http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html.

5.35 We welcome the data handling training programmes Sir Gus O'Donnell[30] has recommended for the civil service, and the more targeted measures recommended by Kieran Poynter[31] in relation to HMRC. We would urge other organisations, including the wider public sector, to consider how to meet this important training need.

5.36 Major decisions about sharing data must be taken at or near the top of the organisation. These cover the key questions of whether, how much, how, and with what safeguards information can be properly shared. Answering them will nearly always require individual judgement. Even here – perhaps especially here – the training and support for top managers may be inadequate. Evidence from the review indicates that in many organisations training is not provided routinely, or at all. To help in this task, organisations need to develop tools and training packages that support individual decision-making. This will involve on the one hand, cultivating a more self-conscious use of professional judgment and thinking about risks and benefits in a structured way; and on the other, fostering a culture that places less emphasis on blame, especially when judgments are based on defensible arguments.

5.37 Sometimes it will be necessary and desirable to empower professionals on the front line to make individual decisions about what information to share, and in what way. As long as the framework is clear, and the process and result are not unreasonable, no one should attempt to usurp that professional's right to make the judgment. The law cannot, and should not, overrule the proper exercise of professional judgement. Rather it should support this by providing a legal framework that respects reasonable judgements based on the circumstances of the case.

[30] http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx. See, for example, paragraph 2.13 *et seq*.

[31] http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf. See, for example, paragraph R16, page 73 *et seq*.

6. Key themes: How to share personal information

6.1 Many of the recent problems with data sharing have been caused by major errors in the actual processes by which data were shared. For example, in the case of the recent loss by HM Revenue & Customs of information relating to some 25 million child benefit records, the sharing of data with the National Audit Office for audit purposes was not in itself contentious. Leaving aside wider leadership, management and cultural issues, the central failures related to the sheer volume of data shared and the processes of sharing. The forensic analysis of this episode recently conducted by Kieran Poynter[32] of PricewaterhouseCoopers illustrates how several interlocking factors – some direct, others of a more general nature – allowed records about 25 million adults and children to be downloaded on to two unencrypted CD-ROMS which were then despatched, through a system that was mistakenly believed to be secure and traceable, from HMRC to the National Audit Office. Reliance on precedence, the many points of contact between the two organisations, a low priority for data security, the failure to use data redaction options, a lack of appropriate authorisations, insecure data storage and transfer methods – all these factors added up to multiple systemic failure and contributed to such a massive data loss[33].

6.2 The themes that emerged during our consultation relating to the 'how' of data sharing may be classified as follows:

- leadership, accountability and culture;
- transparency; and
- technology.

Leadership, accountability and culture

> 'We need to generate the same culture around data protection as for health and safety using the sort of model in their five steps to success: policy, organisation, implementation, audit and measurement.'
>
> **Patients Information Advisory Group**

6.3 Many organisations – both public and private – appear to lack clear lines of responsibility and accountability for the handling of personal information, a problem compounded where information is shared between two or more organisations. We found that although the importance of handling personal information appropriately and securely is widely recognised, all too often good intentions are undermined by a lack of visible senior leadership or accountability structures. In contrast to the United States, where a growing number of chief privacy officers have been appointed at senior level, the

[32] http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf.
[33] Also see, for example, the report into the loss of Ministry of Defence personal data under the Sir Edmund Burton Review and the MOD's action plan in response to the Burton Report: http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm.

post of data protection officer in the United Kingdom is frequently accorded to relatively junior members of staff who have limited ability to assert influence or effect a change in attitude across an organisation.

6.4 In discussion, unflattering comparisons are made frequently between the generally poor culture and accountability for the management of personal information, and the much better culture and accountability for health and safety, and for financial probity. In all organisations, accountability for both health and safety and financial probity, controls and disciplines is seen to rest with the chief executive and the board. This is not usually the case for the handling of personal information. Yet the proper handling of personal information should be instilled into an organisation's psyche in just the same way as health and safety, and sound accounting principles. We were particularly impressed with some of the online and retail companies that we spoke to, where it is clear that the strong message from the top was that respect for personal information is a key part of everybody's job, is the subject of regular training and may be linked to employees' annual bonuses.

6.5 Sir Gus O'Donnell has set out his recommendations[34] to strengthen accountability in central government departments and executive agencies. He recommended that responsibility for handling personal information should rest with permanent secretaries and chief executives. He also proposed standardised and enhanced processes for managing a department's information risk, setting out responsibilities for key individuals; and a role for the Cabinet Office in maintaining and updating minimum mandatory measures. We wholeheartedly endorse these recommendations and support his efforts to encourage and persuade the wider public sector to implement them.

Transparency

6.6 Improving transparency about the extent and nature of sharing of personal information is an important measure that could improve knowledge and trust, allay suspicions about the nature of data sharing and stimulate public debate.

> '*Transparency provides a critical and commendable check over government personal data management, and goes a long way towards dispelling citizens' fears about data sharing problems*.'
>
> **Privacy Enterprise Group**

6.7 When people give their personal information to a public body, a charity or a commercial business – especially if they agree to that information being shared with other parties – they have a right to expect that they will be told the purposes for which their information will be used, who will use it, with whom it will be shared, how long it will be retained, and how it can be updated. They further have a right to expect that their

34 http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx

information will be handled fairly and securely, and that they will be told all this in a clear and straightforward manner, free from excessively legal or confusing language. In short, they have a right not to be taken by surprise on discovering that their information is being used for something wholly unrelated to the original transaction, or by someone who has no business using it or should not have access to it. Yet all too often, they know little or nothing of this and have relatively limited means to find out more. This must be remedied.

6.8 Greater transparency can be achieved in a number of ways. First and perhaps foremost, the approach organisations adopt towards the 'fair processing' or privacy notices is important. We have seen countless examples of privacy notices that are obscured by their length and language. Privacy notices should be written for public consumption, should be genuinely informative and understandable to their target audience. Privacy notices drafted in anything other than concise, plain and straightforward language are unhelpful, and virtually guarantee they will rarely, if ever, be read. Many data controllers need to improve the way they explain their use of personal information to the general public.

6.9 Further, people need to be able to see what information is held about them, and be aware of the rights they have to correct any errors that may exist. The Data Protection Act governs a well-established system of 'subject access requests', by which people can obtain a copy of the personal information that individual organisations hold about them. Public awareness of this right is high: in 2004, a survey commissioned by the Information Commissioner's Office found that 74 per cent of people were broadly aware of their subject access rights, and by 2007 that figure had risen to 90 per cent[35]. There is, however, clear scope for organisations to improve their practices in this area, using technology, where sensible and helpful, to provide increased real-time access and greater transparency. Moreover, organisations – particularly in the public sector – should do as much as they can to allow people to update their records or correct inaccuracies quickly and easily. It is, after all, in the interests of both parties to do so.

6.10 Many data controllers[36] who responded to our review felt that some subject access requests can entail disproportionate effort, particularly when requests appear to be vexatious in nature. While we understand their concerns, and accept that requests can indeed be vexatious and disproportionate in some instances, people's access rights must be upheld. The public should be educated not to abuse the system – but allowing organisations to escape their duty to provide subject access would, in our view, be a step in the wrong direction. Greater openness about the personal

[35] See paragraph 7.2.3 (page 15) of the ICO's Report on Annual Track (2007), prepared by SMSR Ltd: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_track_2007_individuals_report.pdf

[36] The term 'data controller' is used by the Data Protection Act to mean 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'. In effect, by using the term, we mean organisations which control the use, sharing or other processing of personal information.

data held, and better standards for holding it, should eventually reduce the need for individual subject access requests.

6.11 A specific area where there is far too little transparency concerns the identification of bodies with whom organisations share personal information. Many companies or charities ask people to tick boxes on their paper or online forms indicating their consent to sharing their information with 'selected third parties'. It is not usually made clear who these third parties are. Similarly, public bodies have a variety of powers to share personal information with other organisations but they rarely publicise the identity of these bodies. We believe that organisations should publish – and regularly update – a list of other organisations with which they share personal information. We believe that such a move would significantly enhance transparency in this area, eventually resulting in higher levels of public trust.

6.12 We acknowledge that improved transparency is unlikely to mean that the majority of people will spend more of their time contacting organisations to find out what is happening with their personal information. However it does mean that someone with the time, competence and know how can scrutinise organisations effectively when their privacy policies and practices are transparent. It is, in this sense, somewhat analogous to audit. Most people do not carry out audits but the knowledge that an organisation is audited is an indirect reason to instil trust in them.

6.13 There are, however, certain particular cases – some types of law enforcement operations, for example – where greater openness about how personal information is collected, used and shared is not the answer. In such cases it is all the more important that a strong culture of accountability and scrutiny is in place to ensure that the personal information is handled with care.

Technology

6.14 Technological advances have had a dramatic impact on data collection and management. Ever larger databases, powerful search and analysis facilities, and the increased (and almost infinite) storage capacity of modern IT systems belong to a very different world from filing cabinets stuffed with paper. It is simple to share, search and interrogate huge datasets electronically, although not so simple to do this safely and securely.

6.15 The power of computerised systems to handle and process enormous datasets will continue to grow rapidly. In parallel, much work is currently underway to develop new algorithms that will enhance the quality and security of data handling and sharing. The challenges in this area will only increase over time – but so should the market's ability to develop and deliver solutions, as the battle continues between those developing and those dedicated to breaching e-security. However, it is clear that organisations can build systems that are highly secure, even if not impregnable. Internet banking, for example, is now established in most corners of the globe as a safe and highly convenient form of commercial activity. Fraud certainly

occurs, but it seems that the online banking system is essentially secure and trusted by most customers. It is of the utmost importance that organisations are alive to the risks as well as the opportunities, and that they use technology to facilitate business benefits, not to drive them. Two key points relate specifically to computer technology. The first concerns the need to foster research in this crucial area of technology, particularly in the areas of transparency, security and privacy enhancement. Second, it would be a mistake to try to mandate a specific security standard, whether based on the ISO 27000 series[37] or otherwise. Rather, there should be a continuously evolving technology of best practice in the use of computer systems as tools to store and share personal information securely.

6.16 Technological capability is also advancing faster than the ability of many organisations to assimilate that capability. Organisations in both the public and private sectors need to develop the skills of their workforce to match the power of modern and evolving technology. It is not enough for senior managers to assume that IT experts have addressed all the risks to an organisation or the personal information being processed.

6.17 In their submissions to the review, respondents identified a number of opportunities for mitigating risk, including the use of risk-assessment frameworks for data sharing, greater monitoring and controlling of data transfers, and encrypting data for transfers and portable devices. Technical solutions exist, but, as Ernst and Young LLP said in its submission to the Review, 'the application of these is often dependent upon a high level of awareness in individuals of the sensitivity of the data they are sharing or processing. Therefore the risks and opportunities will be relative to what is held, by whom, and for what purpose'.

6.18 Although they can carry new risks, computerised systems can also provide new safeguards for the handling of personal information – controls on access, for instance. The point was made during consultation that sensitive medical records were commonly found lying around on trolleys in hospitals. But whereas a hospital trolley may put at risk scores of records, a data breach affecting a large database (although more secure than a typical hospital trolley) could compromise the security of thousands, hundreds of thousands, or even millions of individuals. HM Revenue & Customs would have found it almost impossible logistically to mislay the records of 25 million customers before the days of digital data storage. Similarly, the low cost of retaining information has made it more attractive in many cases to retain information that would previously have been discarded, further adding to concerns about data security. Nevertheless, technology, when used correctly, can provide greatly enhanced security and safeguards for personal information. Research projects are now able with some ease to work with

[37] The International Organisation for Standardisation (ISO) 27000 series. This is an information security framework, recognised increasing around the world. As the Poynter Report (Chapter XI) concludes, 'implementing ISO27000 strengthens an organisation's information security control processes in a structured way, though of course, effective measures also need to be applied to the controls put in place'. However mandating a specific standard is too inflexible, and the value of such frameworks lies more in their worth as guidance.

anonymised or coded information, where only a few designated people are given access, subject to strict controls, to the facility to link a project code with an individual. There are many examples of where this works well, particularly in statistical research, where a system for accrediting researchers as 'trusted third parties' and secure environments for coding and handling data, known as 'safe havens', have become well established in recent years.

6.19 In summary, it is clear that computerised technology for the processing of personal data brings with it opportunities and risks, and a whole set of new challenges. In our view, however, one principle stands out most clearly: information sharing should be facilitated by technology, not driven by it. The tail should not be allowed to wag the dog. The fact that technology allows more information to be collected about more people does not mean that more information should be collected. Just because something is possible does not mean that we should rush to do it. Benefits can be pursued from collecting personal information and using it appropriately, but there must be an equal focus on safeguards.

Cultural barriers to appropriate data sharing

6.20 Legal barriers to information sharing are often in place for good reasons and serve to prevent inappropriate access or disclosure of people's personal details, such as HM Revenue & Customs strict statutory duty to maintain taxpayer confidentiality.

> 'In our experience, the legal boundaries to information-sharing are often perceived by some in the research community and some staff in the NHS as an unnecessary burden rather than serving the purpose of safeguarding the confidentiality of patient information. It is essential this misunderstanding be addressed.'
>
> **Patients Information Advisory Group**

6.21 Nevertheless, we received evidence that necessary, proportionate and above all, beneficial information sharing is at times frustrated, although there were few specific examples of situations where essential data sharing was being prevented by the legal framework. Indeed, in its submission to the review, the Welsh Assembly Government stated that 'We have always found a basis for sharing personal information where it is considered necessary'. The barriers, therefore, are most often cultural or institutional – an aversion to risk, a lack of funds or proper IT, poor legal advice, an unwillingness to put the required safeguards in place or to seek people's consent. Professor Brian Collins said in his submission to the review that it 'is not so much the *processes* of sharing [that acts as a barrier]… it is the *perceptions* of risk by all parties that will come from actually attempting to do so'.

6.22 Failings within institutions themselves therefore often stand in the way of appropriate information sharing. Formal agreements or practices for information sharing may not be in place or consistent across a sector. Uncertainties about what information can be shared and with whom, and

about what information is actually required, can often result in a default position to withhold information.

6.23 As an example, a lack of clarity and formal arrangements between agencies for sharing information has in some cases obstructed the effective sharing of information in emergencies[38, 39]. Local responders have a statutory responsibility under the Civil Contingencies Act 2004 (CCA) to prepare for emergencies. Part of this requires responders to share information to enable all agency partners to prepare for, respond to and recover from emergencies. In emergency situations, effective data sharing can be hindered by a lack of pre-agreed data sharing protocols between emergency responders, as well as a misunderstanding of what the Data Protection Act does or does not allow in situations like this. These problems are exacerbated by the pressure and urgency placed on responders in emergency situations. Yet the sharing of information underpins all the activities needed to manage an emergency in a co-ordinated way.

6.24 This can also be problematic in cross-sectoral sharing. For example, 'third-sector' organisations including charities and voluntary groups are increasingly working in partnership with central and local government to deliver services for the public, such as children's services, care for elderly people and shelter for those who are homeless. Yet some organisations have reported that they are at times hampered in providing contracted services as a direct result of being denied access to all the information they require, even in situations where public authorities would have a duty to share that information if they themselves were delivering the service.

6.25 For example, when the NSPCC was commissioned by Youth Offender Teams (YOT) to undertake assessments of young people who had received 'final warnings', or 'referral', 'supervision', or 'detention and training' orders for sexually harmful behaviour, in certain cases the NSPCC was unable to obtain prosecution evidence to inform this work. Despite YOT good practice guidance recommending that this information is necessary to these assessments, a Crown Prosecution Service local office felt unable to share it with the NSPCC, on the grounds that the NSPCC did not have a statutory duty to undertake this work.

6.26 Basingstoke and Deane Borough Council said in its submission, the problem is 'that we are all supposedly in the same game but everyone has different rules'. Specifically, the application and understanding of the DPA is not always consistent, and as we have seen, some interpretations of the DPA have turned it into a barrier to information sharing, rather than a means of ensuring that sharing meets appropriate standards. In addition, the question of whether an organisation has the legal power to access or share information is one that clouds many information-sharing initiatives, especially

[38] *Addressing Lessons from the Emergency Response to the 7 July 2005 London Bombings* http://security.homeoffice.gov.uk/news-publications/publication-search/general/lessons-learned
[39] *Data Protection and Sharing – Guidance for Emergency Planners and Responders. HM Government* http://www.ukresilience.gov.uk/preparedness/~/media/assets/www.ukresilience.info/dataprotection%20pdf.ashx

in relation to personal information held by the public sector. And many respondents cited confusion over whether such powers exist as the key factor in preventing information sharing or making the process slow and complex.

6.27 This confusion, and the resulting lack of confidence, needs to be tackled. In Chapter 8 we make recommendations aimed specifically at improving the culture within organisations, and reducing the complexities inherent in the legal framework. We are reassured in making these recommendations by the conclusions reached by the various other reviews that were concluded very shortly before we finalised this report.

7. Powers and resources of the regulator

7.1 A large majority of contributors to the review expressed the consistent and strongly held view that the Information Commissioner and his Office (ICO) have neither adequate powers nor sufficient resources to promote or enforce proper information management practices.

> 'The enforcement mechanisms for the DPA are insufficient: breaches that may cause considerable suffering for individuals, such as damaged credit reference histories, rarely result in any meaningful penalty for data controllers.'
>
> **The British Computer Society**

7.2 The role of the Commissioner, and the ICO more generally, was recognised by consultees as being important for educating and influencing the public and organisations, promoting good practice and providing information and advice; for resolving complaints from individuals; and for enforcing the law by applying legal sanctions against those who ignore or refuse to accept their obligations.

7.3 The Commissioner's Data Protection Strategy, which was adopted after extensive consultation, promotes a society 'in which organisations inspire trust by collecting and using personal information responsibly, securely and fairly'. The Strategy endorses a risk-based approach aimed at minimising the risks for individuals and society when personal data are collected and used; both its approach and priorities are based on maximising the effectiveness of existing powers and resources. But for a regulatory system to bite properly, it must have teeth – and it is clear that the ICO's teeth need to be made sharper. Over the course of our review, we received many calls for greatly increased powers, including additional and strengthened criminal sanctions. Many stated their view that strong action is needed to make sure that people treat personal information in a way that reflects its value.

Powers of investigation, inspection and enforcement

7.4 Under the Data Protection Act, the Information Commissioner has a number of powers to investigate, inspect and enforce organisations' compliance with the data protection principles. Details of these can be found in *Annex H*.

7.5 There have been two recent developments relating to these powers. First, the Prime Minister announced on 21 November 2007 that the Commissioner would be able to carry out (non-statutory) spot checks of government departments. That commitment was reaffirmed by

> 'The problem is the lack of enforcement powers of the Information Commissioner's Office (ICO) which means that organisations have in the past believed that if they breached the DPA the consequences would not be serious.'
>
> **The Direct Marketing Association (UK) Limited**

Sir Gus O'Donnell in the Data Handling Review's final report. Sir Gus made clear in that report the Government's desire to encourage a similar approach throughout the wider public sector. Second, the Criminal Justice and Immigration Act 2008 amended the Data Protection Act, giving the Commissioner the power – yet to be brought into force – to impose civil penalties on any data controller (public or private) for breaching the data protection principles deliberately or recklessly in ways that are serious and likely to cause substantial damage or distress.

7.6 We received an overwhelming body of evidence that the Information Commissioner's existing regulatory powers are too weak for him to carry out his job as effectively as he should. Our attention was regularly drawn to the stark difference between the powers available to other regulators, such as the Financial Services Authority's (FSA), and those of the ICO – not least by the FSA itself.

7.7 The FSA has powers to levy very large penalties on financial services providers found to be careless in their handling of the information for which they are responsible. By contrast, the ICO has traditionally had no powers at all to impose penalties, and it is not yet clear how the new arrangements will work or when they will come into force. For many data controllers, the cost of implementing proper information management systems has far outweighed the likely cost of any regulatory action that might be taken against them. Many organisations, including the FSA itself, have pointed to the unfairness of the current regime that can penalise financial services firms for the errors they make, while other organisations may be handling even more sensitive personal information, for example health and criminal records, and we believe there is a compelling case for levelling the playing field. In its submission to us, the FSA wrote the following:

'The sanctions and powers of the FSA exceed those of… the Information Commissioner's Office. In our view, this may lead to poorer standards of data security in non-financial services firms. This, in turn, could lead to the targeting of the non-financial services firms by criminals seeking to acquire personal information in order to commit fraud and/or identity theft.

'The FSA can both inspect financial services firms without consent and impose fines where an investigation shows that the FSAs rules or principles have been breached… We would strongly support a change in legislation which would give the ICO such powers.'

7.8 Key to promoting and enforcing standards of good practice is the regulator's ability to obtain relevant information from a regulated body. Lessons learnt from data loss incidents within HMRC, Ministry of Defence and elsewhere demonstrate how an organisation's governance, policies, procedures, systems, technology, communications and staff training all contribute to success or failure in the handling of personal information. To process large volumes of personal information successfully demands audit scrutiny in all these aspects. The internal driver of enlightened self-interest should be largely responsible for promoting high standards of data protection, supported by self-assessment. When personal information is shared,

external regulatory scrutiny is even more critical as it may be necessary to examine what is happening inside two or more separate organisations. While regulatory inspections and audits should be consensual wherever possible, the *Principles of Better Regulation* states that any regulator must deploy a mix of carrots and sticks to maintain standards at a consistently high level, and a realistic threat of regulatory inspection, spot checks or audit keeps organisations on their toes. Compulsion should, however, only be introduced as a last resort.

7.9 On investigatory powers, therefore, we believe that it is important that inspections should not have to depend on the consent of the data controller. Furthermore, we consider it an anomaly that there is at present no explicit power requiring a data controller to submit to the scrutiny of an independent inspector or auditor. The regime of spot checks being introduced for central government departments needs statutory authority if it is to be viable and sustainable, and we note that the commitment to extend the regime across the rest of the public sector has yet to be fulfilled. Distinguishing between public, private and voluntary sectors makes little sense, especially as more information is shared across sectors whose boundary lines are forever shifting. However, we also feel that a power to inspect premises or equipment based upon a search warrant – with its association of criminality – is confrontational and at the same time of limited value if it does not permit observation of wider or longer-term aspects of data processing. Moreover, a warrant can be issued only when the court is satisfied that there is already evidence of substantial cause for concern.

7.10 In this light, we echo the call of the House of Commons' Justice Select Committee which, in its First Report of 2007/8[40] – published in January 2008 – urged the Government introduce legislation quickly to provide the Information Commissioner with the powers he needs.

Resources of the ICO

7.11 As the independent regulator, the Information Commissioner's Office requires the resources to perform its regulatory functions. The current funding arrangement for the ICO has not changed since the 1998 Act came into force in 2000. Over time, however, the demands upon the ICO from the rapidly developing information society have increased dramatically, which has consequently stretched its resources. It is clear from our review that the ICO urgently requires additional funding to carry out its current and future duties – a view widely supported in the consultation – and we urge the Government to take swift action to introduce new funding arrangements.

7.12 The ICO's data-protection responsibilities are funded entirely by fees paid by data controllers when they notify details of their processing to the Commissioner. The ICO uses these details to maintain a register of data controllers, which is available for public inspection. The notification

[40] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf

requirements are much criticised by data controllers, but we believe a basic register of data controllers provides a degree of public transparency in holding data controllers to account and helps the Commissioner do his job.

7.13 The notification fee is set by regulations under the DPA at a flat fee of just £35.00 per annum per data controller, a level unchanged since 2000 and irrespective of the controller's size or the amount of regulatory activity it generates. Notification fee revenue in 2006-07 was £10.2 million, with which the ICO must carry out all its regulatory and advisory duties in respect of some 300,000 data controllers. This level of funding contrasts poorly with that available to other regulators with similar duties and has in part resulted in the regulator's inability to make the best use of its existing powers. Recent developments have already substantially increased demands and expectations, and it is clear to us that increasing powers and responsibility must go hand in hand with increased resources. We are pleased to report that that funding discussions between the ICO and the Ministry of Justice are now well advanced and in Chapter 8 we make some specific recommendations about how the funding arrangements should be improved, particularly through the introduction of a multi-tiered system.

Conclusion

7.14 We believe that the Information Commissioner has insufficient powers and resources to carry out his duties as effectively as possible. This has given the impression that the Government accords little priority to the proper handling of personal information. This may be a misconception, and we welcome the Government's commitment to strengthening the Commissioner's powers and sanctions and to ensuring that his office receives greater funding to carry out its duties. However, to further counter the worrying impression that it cares little about safeguarding personal information, we urge the Government to act swiftly to adopt a focused and coherent package of measures aimed at strengthening the Information Commissioner's authority and giving bite to his enforcement powers.

8. Recommendations

8.1 The case for change is strong. The law and its framework lack clarity, responsiveness and bite. Public confidence is evaporating and technology continues to advance. While there can be no quick or easy solutions, a package of clearly targeted measures could radically transform the way personal information is collected, used and shared. We believe change is necessary in five areas, namely:

- to transform the *culture* that influences how personal information is viewed and handled;
- to clarify and simplify the *legal framework* governing data sharing;
- to enhance the effectiveness of the *regulatory body* that polices data sharing;
- to assist important work in the field of *research* and statistical analysis; and
- to help safeguard and protect personal information held in publicly available sources.

Box 5: Ground-rules
We have developed some simple ground rules that we think aid sound decision making about sharing personal information. While clearly not intended to replace the specific requirements of data protection law or the data protection principles, these ground rules have informed our approach and recommendations, and they summarise our view of the core considerations for using and sharing personal information:

- Organisations must have effective controls in place, setting out clear lines of accountability and aiming for maximum transparency, to safeguard the personal information they hold and share.
- In line with the principle of minimising the amount of data collected and used, organisations should collect and share only as much personal information as is essential and store it only for as long as is necessary.
- Organisations must train their staff to understand the risks of handling personal information and to meet the reasonable expectations of those whose data they hold, and of the regulator.
- Whether or not personal information should be shared can be considered only on a case-by-case basis, weighing the benefits against the risks.
- The case for sharing personal information will usually be stronger when it brings clear benefits, or when *not* sharing personal information may risk significant harm.
- The sharing of personal information should be adequately documented and subject normally to privacy impact assessments.
- When organisations share personal information, they must pay particular attention to these inherent risks: perpetuating or exaggerating inaccurate or outdated data; mismatching data; losing data; and intruding excessively into private lives. This becomes even more critical when entire databases are shared.

I Cultural changes

Introduction

8.2 It is clear to us that data sharing is shrouded in confusion. This, in turn, has given rise to a culture that is risk averse. The fact that we encountered few examples of insurmountable barriers suggests that decisions are eventually being made, but only after much agonising. We believe that this is unacceptable.

8.3 The organisational culture of those who collect, manage and share personal information needs to change. While the past few decades have witnessed major improvements to corporate governance arrangements in some sectors, many organisations - in the public sector especially - have not similarly improved governance in their handling of personal information,

8.4 Sharing information carries both benefits and risks, as do all types of processing. But the culture of indecision that surrounds data sharing is problematic and needs to change, particularly in the public sector.

8.5 This change must go hand in hand with a wider shift in cultural values, viewing personal information as an asset to be treated with respect. These are leadership matters, as reports[41] from Sir Gus O'Donnell and others stress. Our specific recommendations aimed at promoting cultural change cover issues of leadership and accountability; transparency; training and awareness; and the way in which organisations can best authenticate entitlement to goods or services using the minimum personal information possible.

Leadership and Accountability

8.6 Leaders in the public, private and voluntary sectors should rise to the challenge, developing the confidence to make and be held accountable for the tough decisions that sharing inevitably entails. They need to be held to account for any failures to make decisions, as well as for the decisions they do take.

8.7 Indeed, strong leadership and clear lines of accountability are key to good information handling. In organisations where the most senior executives take a prominent role in shaping corporate standards, and where information is considered a valuable asset, the culture is invariably more attuned to the importance of good information-handling practices. In such cases, the people at the top take ultimate responsibility for the way information is handled, used and shared.

8.8 We support Sir Gus O'Donnell's moves[42] to ensure that Permanent Secretaries and Chief Executives of central government departments and

[41] See paragraph 1.13, above (footnote 9)

[42] http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx

agencies are responsible and accountable for the handling of personal information. We especially welcome the new requirement that, as Accounting Officers, they should explicitly reflect assessments of information risks in their annual Statements of Internal Control. We support Sir Gus's efforts to persuade the wider public sector to implement similar measures.

8.9 Personal information is a valuable asset for any organisation and needs proper safeguards. There are reputational and other risks if things go wrong, but the greatest risks are usually faced by the individuals concerned. We feel strongly that all organisations handling personal information – both in the public and private sectors – need robust leadership and accountability mechanisms to ensure that this is done well.

8.10 ***Recommendation 1***: **As a matter of good practice, we therefore *recommend* that all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information**. This should normally be at senior executive level, giving a designated individual explicit responsibility for ensuring that the organisation handles personal information in a way that meets all legal and good-practice requirements. Audit committees should monitor the arrangements and their operation in practice.

8.11 ***Recommendation 2***: **We further *recommend* that as a matter of best practice, companies should review at least annually their systems of internal controls over using and sharing personal information; and they should report to shareholders that they have done so.** The Combined Code on Corporate Governance[43] requires all listed companies to review 'all material controls, including financial, operational and compliance controls and risk management systems'. The recommended processes for identifying, controlling and monitoring key risks are elaborated in the so-called Turnbull Guidance[44]. Recent events – in the public and private sectors – can have left no doubt that any company handling significant amounts of personal information faces major risks and that adequate internal controls – both 'operational' and 'compliance' – are essential. It would be surprising and worrying not to see information risks

[43] http://www.frc.org.uk/corporate/combinedcode.cfm.
[44] http://www.frc.org.uk/corporate/internalcontrol.cfm.

addressed explicitly in the Statements of Internal Control for such companies. We hope that bodies such as the Confederation of British Industry will develop guidance to help companies ensure their controls and disclosures are adequate. If approaches on these lines are not successful in improving high-level accountability for giving assurance on information risks, we would expect the Financial Reporting Council to intervene.

Transparency

8.12 People rightly expect to know why their personal information is held and for how long, how it is kept safe, with whom it is shared, and whether and how they can access it to check and/or update it. It is clear that organisations need to be more open and transparent about their data-sharing activities. In particular, they need to be far more transparent about *how* they acquire personal information, *what* they use it for, *who* has access to it, *with* or to *whom* they share or sell it, and *how long* they retain it. We believe strongly that it is in organisations' own interest to do so.

8.13 Only when people better understand what happens to their personal information will they invest more trust in the organisations that process it. And only when levels of trust are suitably high will organisations be able to take full advantage of the potential benefits offered by the use of personal information, passing on those benefits to the public through more efficient, better-value services.

8.14 ***Recommendation 3***: **We therefore *recommend* that organisations take the following good-practice steps to increase transparency**:

(a) **Fair Processing Notices should be much more prominent in organisations' literature, both printed and online, and be written in plain English. The term 'Fair Processing Notice' is itself obscure and unhelpful, and we recommend that it is changed to 'Privacy Policy'**.

(b) **Privacy Policies should state what personal information organisations hold, why they hold it, how they use it, who can access it, with whom they share it, and for how long they retain it**. The policy can be best set out using a 'layered' approach. This

involves preparing a relatively simple explanation backed up by a more detailed version for people who want a more comprehensive explanation.

(c) **Public bodies should publish and maintain details of their data-sharing practices and schemes, and should record their commitment to do this within the publication schemes that they are required to publish under the Freedom of Information Act**.

(d) **Organisations should publish and regularly update a list of those organisations with which they share, exchange, or to which they sell, personal information, including 'selected third parties'**.

(e) **Organisations should use clear language when asking people to opt in or out of agreements to share their personal information by ticking boxes on forms**. At present, companies often switch from positive to negative questions on the same page. In particular, firms operating online should be much more open about what customers are signing up to, and what their policies are for retaining and sharing personal information.

(f) Proper data management requires that individuals are able to inspect, correct and update their own data. This is also in the self-interest of any organisation that relies on or values accurate information. **Organisations should do all they can (including making better use of technology) to enable people to inspect, correct and update their own information – whether online or otherwise**[45]**.**

Training and Awareness

8.15 Systems and processes are, of course, only as strong as their weakest link. If an organisation is to handle information well, *all* individuals within it must

[45] As Professors Charles Raab, Perri 6 and Christine Bellamy say in *The Glass Consumer* 'One of the advantages of the development of on-line facilities for service users to exercise their right to know what is held about them might be that, at a trivial cost, they could provide users with individualised information about the sharing of their personal data, on a routine and automatically generated basis.' This was published in 2005. As online technology makes rapid advances, the point is even more pertinent today. See: *The Glass Consumer: Life in a Surveillance Society*, Chapter 5, edited by Susanne Lace, published by Policy Press (14 June 2005).

know what is expected of them. In particular, they must understand how to use and share personal information securely and appropriately. Aside from instances of actual dishonesty, most breaches or misuses of information result from human error. Education and training for employees – and for the public more generally – is vital to increasing awareness and improving compliance.

8.16 Other countries have established successful programmes to develop expertise across the market place. For example, the International Association of Privacy Professionals runs an education programme in the United States of America that certifies practitioners as having attained particular standards in the information and privacy sphere. Three-year certification is awarded to those who undertake training in the essentials of U.S. and international privacy and data protection laws, standards and practices and then pass relevant examinations. They must also maintain a minimum of some ten hours of continuing professional training per year throughout the three-year term. Levels of certification vary according to need, and a similar scheme exists in Canada.

8.17 ***Recommendation 4***: **We therefore *recommend* that all organisations routinely using and sharing personal information should review and enhance the training that they give to their staff on how they should handle such information**. Organisations should develop incentives to encourage better understanding and avoid errors, without developing a culture of blame that results in people covering up their mistakes. Learning from mistakes is a crucial part of the learning process, and openness within an organisation helps it to be honest with its customers when things go wrong. It is important that people working with personal information understand that the information they handle is potentially sensitive and important, both to the individuals concerned and to the organisation, and that high professional standards are required at all times and at all levels. In particular, staff working with personal information must recognise that they are the guardians of that information.

Identification or authentication?

8.18 Changing the culture will also involve looking at why information is collected. A clear distinction exists between *identification* and *authentication*. When all you need to prove is that you are entitled (or have the appropriate credentials) to access a service or buy a product, then it is unnecessary to prove who you are, merely that you have the relevant credentials. For example, it would be wrong to be required to provide your name and address in order to go to a film with an over-18 certification, when all you should need to prove is that you are over the minimum age. But too often,

credentials and identity get conflated, and as a result, more personal information is collected than is absolutely necessary. This breaches the data protection principles and should cease.

8.19 ***Recommendation 5*: We therefore *recommend* that organisations should wherever possible use authenticating credentials as a means of providing services and in doing so avoid collecting unnecessary personal information**.

II Changes to the legal framework

Introduction

8.20 When personal information is to be shared, we believe there is a lack of clarity about what the law permits or prohibits. This needs to change. The recommendations we make about the prevailing culture will be crucial. But we believe that changes to the law are also required, not least because they should help to embed the necessary new attitudes to personal information within organisations' hearts and minds.

8.21 A significant problem is that the Data Protection Act fails to provide clarity over whether personal information may or may not be shared. The Act is often misunderstood and considerable confusion surrounds the wider legal framework – in particular, the interplay between the DPA and other domestic and international strands of law relating to personal information. Misunderstandings and confusion persist even among people who regularly process personal information; and the specific legal provisions that allow data to be shared are similarly unclear.

8.22 Our terms of reference were limited to reviewing the operation of the Act rather than the Act itself. This is because the Act is very tightly tied to the EU Directive on the protection of personal data, which leaves only limited scope for flexibility. However, the Information Commissioner's Office has recently awarded a contract to RAND Europe to conduct a review of EU data protection law and the European Commission is also seeking tenders to conduct a comparative study on privacy challenges in the light of new technology. We welcome both these initiatives. Neither constitutes an official EC review of the Directive, but we trust that such a review will follow in due course.

8.23 Within the scope of our review, we nonetheless believe that worthwhile reforms are possible in the shorter term, both to help reduce confusion and to increase the law's responsiveness in situations where unnecessary barriers exist. Our recommendations therefore call on the Government to bring forward legislation in the next parliamentary session to achieve these aims.

Review and reform of the EU Directive 95/46/EC

8.24 Throughout the review, EU Directive 95/46/EC on the protection of personal data was the subject of much criticism. As a prime source responsible for much of the confusion in the UK's Data Protection Act, especially surrounding the definition of personal data, it is clearly ripe for reform.

8.25 ***Recommendation 6***: **Any changes to the EU Directive will eventually require changes to the UK's Data Protection Act. We recognise that this may still be some years away, but we nonetheless *recommend* strongly that the Government participates actively and constructively in current and prospective European Directive reviews, and assumes a leadership role in promoting reform of European data law**.

8.26 First, this will shake off any impression that successive governments have been lukewarm about data protection. But more importantly, as data flows become ever more global, the Government has the opportunity to provide leadership in this area by advocating practical international approaches to data protection, rather than simply responding to the proposals of others.

8.27 The United Kingdom has a strong case to make for its own more flexible approach to data protection matters – particularly in the light of technological developments that reduce the relevance of national boundaries. Any revisions to the Directive will flow through to a revised UK Data Protection Act. That alone is sufficient reason for the Government to influence the debate as much as possible.

Statutory Code of Practice on data sharing

8.28 The need for consistent and clear guidance to data controllers has never been more important. Practitioners currently rely on a plethora of guidance from many sources. Of varying quality, much of it is piecemeal and outdated, frequently unread or apparently in conflict with other guidance. Overall, it neither relates to the situations people face in their daily lives, nor stands up to close scrutiny. This inevitably adds to the confusion and uncertainty practitioners experience when considering whether or how to share personal information.

8.29 The Information Commissioner's Office is the obvious place to seek clarity on matters relating to personal information, but it has not enjoyed sufficient authority or influence in relation to data sharing, especially in its dealings with public bodies. Although it has done much in recent years with its programme of guidance, the ICO has recognised that, until recently, its published guidance on sharing was neither as sharp nor as focused as it might be. Guidance must be comprehensive, clear and authoritative, and it must inspire confidence in practitioners.

8.30 ***Recommendation 7(a)***: **We *recommend* that new primary legislation should place a statutory duty on the Information Commissioner to publish (after consultation) and periodically update a data-sharing code of practice. This should set the benchmark for guidance standards**.

8.31 ***Recommendation 7(b)***: **We further *recommend* that the legislation should provide for the Commissioner to endorse context-specific guidance that elaborates the general code in a consistent way**.

8.32 The ICO's *Framework Code of Practice for Sharing Personal Information* – published in 2007 – should be the starting point for this statutory code and we anticipate that, subject to consultation, the final code will closely follow this model. The existing framework code is reproduced as *Annex G*.

8.33 A statutory code of practice would not eliminate the need for further context-specific guidance, but would establish a central reference point from which further, more consistent guidance could be derived.

8.34 We believe that creating a separate and explicit duty would provide greater clarity and introduce greater scrutiny. In particular, we consider it vital to provide that the general code is laid before – and approved by – Parliament. This would be in keeping with similar codes in other fields[46] but cannot be achieved through section 51 of the Data Protection Act.

8.35 The code of practice should:

- establish standards setting out how organisations involved in sharing personal information should handle and protect the data under their control; and
- apply to all those involved in data sharing, who should adhere to it as a matter of good practice and consider it as an authoritative interpretation of the relevant data protection principles.

8.36 We would envisage that, when setting out best-practice standards, the Commissioner's Code should encourage the wider use of privacy impact assessments, for example.

[46] See for example the ACAS *Discipline and Grievance at Work* guidance, established under s.207 Trade Union and Labour Relations (Consolidation) Act 1992

8.37 Although we recognise that a transitional period will be necessary to allow adjustments to non-compliant arrangements, the code would govern both current and future sharing arrangements.

8.38 While breach of the code should not be against the law in or of itself, the code should have suitable authority and be sanctionable in the sense that the Commissioner and the courts should be expressly entitled to take non-compliance with its provisions into account when deciding whether data controllers have complied with the data protection principles. As a corollary, compliance with the code would reassure organisations that they would not face enforcement problems. With this degree of statutory authority, the code must obviously be drawn up in a way that is consistent with the EU Directive and other international obligations.

Overcoming legal obstacles and absent powers

8.39 Although we found the most significant barrier or hindrance to effective data sharing to be legal uncertainty and confusion, there are occasions when real legal obstacles – either statutory or common law prohibitions, or the absence of the necessary legal power – inhibit the sharing of data.

8.40 We are mindful that many express prohibitions exist for good reasons, whether they appear in statute or elsewhere. But we have also seen a few examples of proposed data-sharing schemes that would be safe and beneficial, but which are currently prevented by the law. Moreover, we have encountered several cases where Parliament has overcome a legal barrier by creating a specific statutory gateway, thereby adding to the proliferation of legislation (both generally and in the field of data protection) and undermining clarity still further. This also makes it harder to scrutinise individual cases. What is needed is a mechanism to consider these cases in a transparent and consistent manner, ensuring greater scrutiny while at the same time reducing scope for confusion.

8.41 ***Recommendation 8(a)***: **We *recommend* that where there is a genuine case for removing or modifying an existing legal barrier to data sharing, a new statutory fast-track procedure should be created. Primary legislation should provide the Secretary of State, in precisely defined circumstances, with a power by Order, subject to the affirmative resolution procedure in both Houses, to remove or modify any legal barrier to data sharing by**:

- **repealing or amending other primary legislation;**
- **changing any other rule of law (for example, the application of the common law of confidentiality to defined circumstances); or**

- **creating a new power to share information where that power is currently absent.**

8.42 Section 75 of the Freedom of Information Act 2000 provides a parallel in this respect. Also subject to the affirmative Parliamentary procedure, this gives the Secretary of State the power to amend or repeal enactments prohibiting disclosure of information. But we believe that data sharing requires additional safeguards aimed at increasing the scope for expert scrutiny on a case-by-case basis.

8.43 ***Recommendation 8(b)***: **We *recommend* that, before the Secretary of State lays any draft Order before each House of Parliament, it should be necessary to obtain an opinion from the Information Commissioner as to the compatibility of the proposed sharing arrangement with data protection requirements**. There should be a requirement that a full and detailed privacy impact assessment would be published alongside any application, to assist both the Information Commissioner and Parliament's consideration.

8.44 When making an Order, the Secretary of State could include necessary conditions and safeguards, addressing in particular any concerns of the Information Commissioner. And because of its exceptional and potentially controversial nature, the Order would be subject to the affirmative resolution procedure.

8.45 We recognise that in its fourteenth report of 2007/8[47], the Joint Committee on Human Rights expressed concerns about the use of secondary legislation to authorise information-sharing schemes. The Committee was particularly concerned about the absence of appropriate protections enshrined in primary legislation, when broad enabling powers are used It concluded that primary legislation should set out the necessary safeguards in each individual case. We agree that robust safeguards are important, but think the system we propose will meet the challenge well.

8.46 First, the new process will be far more transparent in the sense that enabling powers will no longer be scattered around the statute book, but passed into law through a simple and easy-to-understand mechanism that anyone can monitor. Second, the role of the Information Commissioner is key. Before any application could be considered, a full and detailed privacy impact assessment would need to be published; and the Commissioner would subsequently publish his opinion, which Parliament could consider in each

[47] UK Parliament's Joint Committee on Human Rights. See http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

and every case. In any event, the protections enshrined in primary legislation by the Human Rights Act and the Data Protection Act will always apply, so any secondary powers used will ultimately be subject to challenge in the courts.

8.47 The authorisation process would not prevent the use of dedicated primary legislation in particular cases of data sharing, if it were considered appropriate for whatever reason. For example, we believe this process would not be appropriate for large-scale data-sharing initiatives that would constitute very significant changes to public policy, such as those relating to the National Identity Register or the National DNA database.

III Regulatory body changes

Introduction

8.48 During the review we heard many calls for the regulatory body to have greater enforcement and inspection powers to reinforce comprehensive and authoritative guidance. It needs sufficient resources to carry out its duties effectively, and to give it the necessary status and influence to regulate and protect personal information.

8.49 We agree with these sentiments and believe that significant changes are necessary to enhance the authority of, and respect for, the Information Commissioner's Office, and to enable it to carry out its duties as effectively as possible. In this section we make recommendations on changes to the sanctions regime, the inspection regime, the resourcing of the regulatory body, and the constitution of the regulatory body.

Sanctions under the Data Protection Act

New civil sanction – section 55A Data Protection Act 1998

8.50 The Commissioner's new power (s.55A DPA) to impose financial penalties on organisations found to be deliberately or recklessly breaching the data protection principles marks a major step forward in creating a robust regulatory environment for information management. Created by the Criminal Justice and Immigration Act 2008, it will have considerable value in its deterrent, educative and punitive effects. The new power was put in place during the course of our review, and we welcome it unequivocally. Its cross-party genesis and support are particularly significant.

8.51 Contraventions of data protection requirements must have been deliberate or reckless and need to be 'serious' before a penalty can be incurred. 'Substantial' damage or distress to the individual must be a likely consequence. It will therefore be justifiable for substantial maximum penalties to be set.

8.52 ***Recommendation 9***: **We *recommend* that the regulations setting out the maximum level of penalties should mirror the**

existing sanctions available to the Financial Services Authority, setting high, but proportionate, maxima related to turnover.

8.53 ***Recommendation 10***: **We also *call on* the Government to bring these provisions fully into force within six months of Royal Assent of the Criminal Justice & Immigration Act, that is, by 8 November 2008**. As well as sending a powerful message underlining the new powers of deterrence, this will significantly strengthen the Information Commissioner's hand.

Breach notification

8.54 Any organisation that handles, uses or shares personal information must employ sufficient safeguards to protect that information from loss or theft. However, no system of protection can ever be completely safe. When data breaches do occur, it is therefore vital that organisations take all necessary steps to manage and mitigate the risk to individuals and to the integrity of the organisation's operations.

8.55 When personal information has been lost, stolen or otherwise compromised, the immediate imperative is to manage the security breach. The ICO has published guidance on this, and well-run organisations will have put in place their own contingency arrangements. Where individuals face a real risk, for example of identity theft or fraud, it will usually be necessary to notify them directly so that they can take mitigating action.

8.56 When an organisation notifies the Information Commissioner's Office of a data breach that carries a risk of substantial harm to individuals, the ICO should advise on what action the organisation should take, based on its assessment of the seriousness of the breach. In cases of imminent and serious risk to an individual, the organisation should inform the individual at the same time as – or even before – it notifies the ICO. Many organisations do this already, and it should be a matter of best practice for all organisations.

8.57 We have considered the suggestion that it should be mandatory to notify the ICO of all serious security breaches. Legislation requiring this can help organisations identify systemic security problems, and motivate them to introduce better security measures to protect personal information. Notification also alerts people whose personal information has been breached to do all they can to prevent identity fraud and theft.

8.58 Laws requiring the notification of data breaches have become commonplace in some other countries, including the United States and Japan. However, we do not favour placing an explicit statutory duty on organisations to report all breaches. Not only would this add a significant extra burden for

organisations but more worryingly, it could produce 'breach fatigue' among the wider public if it were to result in frequent and unnecessary notifications of minor incidents. This carries the very real danger that people will ultimately ignore notifications when there is, in fact, significant risk of harm.

8.59 ***Recommendation 11***: We believe that as a matter of good practice, organisations should notify the Information Commissioner when a significant data breach occurs. We do not propose this as a mandatory requirement, but **in cases involving the likelihood of substantial damage or distress, we *recommend* the Commissioner should take into account any failure to notify when deciding what, if any, penalties to set for a data breach**. Updated guidance should make this clear.

8.60 This should encourage good practice while leaving the initial decisions to the relevant data controller. It recognises that each breach carries different levels of risk and, consequently, requires a different response.

Inspection and audit powers of the regulator

8.61 The key to effective enforcement lies in the regulator's ability to undertake necessary investigations and inspections, so that regulatory failures can be identified and corrected. The possibility or threat of external scrutiny will do much to encourage organisations in the public, private and voluntary sectors to take compliance seriously. In those cases where there is resistance the power to inspect will need mandatory back-up. Indeed, without an incentive or legal compulsion, it is doubtful that many organisations would want to take the risk of consenting to an inspection. The need for effective powers of inspection was almost universally accepted by our respondents. It is needed to be certain of UK compliance with the EU Directive and was endorsed in January 2008 by the Justice Committee Report on the Protection of Personal Data[48].

8.62 During the course of our review, we were directed to the provisions on regulatory inspections in the Republic of Ireland's Data Protection Act. We understand that these work well. Section 24 of the Irish Act is set out in full in *Annex I*[49]. In summary, it allows an authorised officer to enter relevant premises to enable the Commissioner to carry out his functions. The authorised officer has the power to:

- enter the premises and inspect any data and any data equipment;

[48] Justice Select Committee's First Report of 2007/8, paragraphs 23 and 29: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf

[49] As well as covering the Irish Act, *Annex H* includes certain other material on international privacy law that we were referred to during the review.

- require the organisation or its staff to help in obtaining access to data, and to provide any related information;
- inspect and copy any information; and
- require the organisation or its staff to provide information about procedures for complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.

8.63 Under Irish legislation, it is an offence to obstruct or impede an authorised officer, or knowingly to give false or misleading information to an authorised officer. We are attracted to this model, in particular because of the flexibility it provides to the regulator. The power needs to be available (1) where the regulator suspects that an organisation is not complying with the law, (2) where the activities or circumstances are such that there may be a risk of non-compliance even though there are not yet any grounds for suspicion and (3) where the regulator needs or wishes to carry out a random check. The Irish model also provides flexibility in the sense that it embraces the full spectrum of activity ranging from a spot check of a particular site or activity, through a more wide-ranging inspection, to a full audit. Moreover, 'processing' data is an on-going activity. To check an organisation's compliance with data protection requirements may take some time, usually on-site, examining how policies, procedures and technologies are operating in practice and checking management and staff behaviours. A good understanding of these matters is also required to shape any follow-up remedial or enforcement action that may be required.

8.64 The possibility of an inspection should be a powerful weapon in encouraging all organisations to comply with their obligations. The threat of an enforced inspection should be sufficient to secure the co-operation of most organisations that come to the regulator's attention, but prove to be recalcitrant. The threat must be real and credible and occasionally it will have to be exercised. However, the power to enter private premises is a strong one and safeguards are essential. Unlike the Irish law, therefore, we consider that a court order should be required to authorise entry to premises against the occupier's wishes. We are sceptical however that this should be modelled on the search warrant powers in Schedule 9 of the DPA. A search warrant can only be obtained in limited circumstances, is more suited to criminal misconduct and is not suitable in cases requiring a fuller inspection than can be carried out on a single visit or by seizing equipment.

8.65 ***Recommendation 12***: **We *recommend* that the Information Commissioner should have a statutory power to gain entry to relevant premises to carry out an inspection, with a corresponding duty on the organisation to co-operate and supply any necessary information. Where entry or co-operation is refused, the Commissioner should be required to seek a court**

order. We emphasise that the *threat* of compulsion should be enough in most cases. In practice, we envisage the system would work largely by consent, but it should employ a progressively tougher approach for situations in which co-operation is not forthcoming, culminating where necessary with the authority of a court order. Such an approach would be more robust and effective than the present arrangements, but we believe this represents a good balance between new powers for the regulator and appropriate safeguards for private individuals and organisations.

Resources of the regulator

8.66 We have argued in the report that the ICO requires more funding as a matter of urgency; this is all the more important if the organisation is to be effective in deploying the proposed new regulatory powers.

8.67 ***Recommendation 13***: **We therefore *recommend* that changes are made to the notification fee through the introduction of a multi-tiered system to ensure that the regulator receives a significantly higher level of funding to carry out his statutory data-protection duties.** The ICO is anticipating additional fee income of £6 million per annum from increased fees, which would enable it to improve its infrastructure and undertake enhanced inspection duties. We believe that such an increase would, at least initially, enable the ICO to modernise and take on additional responsibilities.

8.68 A multi-tiered notification fee would reflect more fairly the cost to the regulator of differently sized organisations, and resolve the perceived unfairness by which individual practitioners who process data about just a few people pay exactly the same fee as large companies or government departments who process the data of millions of people.

8.69 A simple two- or three-tiered scale, differentiating for example between large, medium and small-sized data controllers, would in our view be the most appropriate structure for a graduated fee arrangement. Depending on where the line is drawn, a tiered scale would probably affect only 10 per cent or fewer data controllers, leaving the vast majority with no or very modest increases. Recent ICO research reinforces our view that increases on these lines would not encounter any serious objections. It is, however, important that the new arrangements are simple and do not impose bureaucratic burdens on controllers or the ICO. We therefore propose that data controllers should assess themselves to determine their correct tier.

Constitution of the regulator

8.70 The package of reforms we are recommending is necessary both to restore confidence in the ability of public, private, and voluntary-sector organisations to handle personal information, and to simplify and clarify the processes so that everyone involved can better understand how the system works. Our package is evidence-based and workable in practice. But it is undeniable that it will change the regulatory landscape: the Information Commissioner's Office will have considerably more powers and responsibilities, and must be resourced accordingly. We need to ensure that the office itself is properly equipped to deal with its new role.

8.71 An important question to address is whether the single commissioner model, as currently exists, is best placed to lead and manage the regulatory body as it moves into a new era. We have come to the firm conclusion that it is not.

8.72 ***Recommendation 14***: **We therefore *recommend* an alternative model in which the regulatory body is re-constituted as a multi-member Information Commission, to reinforce its status as a corporate body**.

8.73 In a speech to the Centre for Regulated Industries in January 2008, Richard Thomas argued that the position of a sole Information Commissioner is somewhat anachronistic. He pointed out that most of the former Directors-General in other areas of regulation were converted to Boards or Commissions some years ago, and that sole regulators are now rare.

8.74 A multi-member commission, rather than a single commissioner, has a number of distinct advantages. The main ones are as follows:

- It would strengthen the influence and authority of the ICO.

- A single commissioner risks personalising the work of the regulatory body too much. The decisions that must be taken are often uncomfortable and unwelcome. The work of the regulator could be damaged if – for whatever reason – the commissioner suffers poor personal or professional relationships with key stakeholders, such as ministers and officials. A multi-member commission reduces this risk.

- Similarly, a single commissioner could find himself or herself subject to significant and, at times, inappropriate pressure from stakeholders. A multi-member commission is more likely to be able to handle such pressures than any single individual, thus strengthening the regulator's independence.

- Although the appointments system has worked very effectively to date, a multi-member commission reduces the risk that a maverick individual

starts to lead the organisation in ways that raise serious concerns among those being regulated and/or the general public, whether in terms of policies, practices or priorities.

- Different commissioners would bring to the regulator the benefits of their diverse backgrounds and skills.

8.75 Our recommendation formalises and builds on the successful arrangements introduced four years ago, under which the Commissioner and his two statutory Deputies are supported by four non-executive Management Board members. Appointed on a non-statutory basis, the latter cannot have any role in regulatory decision-making. Unless formalised, there is also no requirement or assurance that this arrangement will continue.

IV Research and statistical analysis

8.76 Research and statistical analyses represent important opportunities for using and sharing information, as discussed in Chapter 2. Developing an evidence base to improve health and social policy in many areas depends on using data derived from collections of personally identifiable material. Wherever possible, such data should be anonymised, but creating anonymised information involves accessing and processing personal information to remove identifiers from it. Many research questions also require the use of coded datasets that no longer contain explicit identifiers, but ultimately allow the data to be linked to a particular individual. Such data are often described as 'pseudonymised'; and preserving these potential identifiers may be vital, for example, to allow the linkage of pseudonymous data about the same person to facilitate a longitudinal study, or for postcode data in cases involving geographically sensitive research questions.

8.77 The aim here is to allow this important statistical and research analysis to proceed, while minimising the risk of identifying individuals from within datasets. In our view, the approach of creating and using coded data should be recognised as a legitimate way of safeguarding people's identities, and that data handled in this way should not constitute a breach of the Data Protection Act.

8.78 A useful device in this context is that of 'safe havens'. These have three key characteristics. The first is that they provide a secure environment for processing identifiable personal data. The second is that only 'approved researchers' can gain access to the data. The third is that there should be penalties for anyone who abuses personal data. There are precedents within the UK and in other Commonwealth jurisdictions for this approach to data handling. For example, in England, the Statistics and Registration Service Act 2007[50] can grant 'approved researchers' access – for the purposes of statistical research – to personal information held by the new Statistics Board. The Board may extend access to researchers from various

[50] See in particular section 39 *et seq.* (http://www.opsi.gov.uk/acts/acts2007/ukpga_20070018_en_3#pt1-pb11-l1g39)

organisations, including academic institutions, public bodies and non-governmental organisations. These researchers are then bound by a strict code, which prevents disclosure of any personal identifying information. Any deliberate or negligent breach of data security by the approved researcher would entail criminal liability and the prospect of a custodial sentence up to a maximum of two years.

8.79 ***Recommendation 15***: **We *recommend* that 'safe havens' are developed as an environment for population-based research and statistical analysis in which the risk of identifying individuals is minimised; and furthermore we *recommend* that a system of approving or accrediting researchers who meet the relevant criteria to work within those safe havens is established. We think that implementation of this recommendation will require legislation, following the precedent of the Statistics and Registration Service Act 2007. This will ensure that researchers working in 'safe havens' are bound by a strict code, preventing disclosure of any personally identifying information, and providing criminal sanctions in case of breach of confidentiality.** We urge Government to bring forward the necessary legislation as soon as possible.

8.80 ***Recommendation 16***: Implementation of recommendation 15 will enable full advantage to be taken of the benefits made possible by safe havens. **We therefore *recommend* that government departments and others wishing to develop, share and hold datasets for research and statistical purposes should work with academic and other partners to set up safe havens**.

8.81 One area of research raises a 'Catch 22' dilemma, however. Researchers may wish to approach individuals in order to gain their consent to participating in a particular piece of research, for example the trial of a new treatment for a particular disease. The issue is how to identify these people in the first place. The requirement for 'consent to gain consent', which is largely limited to medical research, is a problem that requires a solution.

8.82 ***Recommendation 17***: **We *recommend* that the NHS should develop a system to allow approved researchers to work with**

healthcare providers to identify potential patients, who may then be approached to take part in clinical studies for which consent is needed. These approved researchers would be bound by the same duty of confidentiality as the clinical team providing care, and face similar penalties in the case of any breach of confidentiality. If legislation is necessary to implement such a scheme, then we would urge Government to bring that legislation forward as quickly as possible.

V Safeguarding and protecting personal information held in publicly available sources

8.83 In Chapter 2, we referred to the recent development and growth of on-line services which aggregate personal information about large numbers of people from publicly available sources – such as the electoral register, company registers, phonebooks and websites. The ready availability of so much information is a worrying threat to privacy, and sometimes to security. In July 2006 - after receiving almost 1600 complaints - the Information Commissioner's Office issued an enforcement notice against the *B4U* website, which offered a free 'people search' facility, using data from the pre-2002 'full' Electoral Roll. Complainants included a police officer whose family's names and address, along with a map to their house, appeared on the website; and an individual who had previously been a victim of identity fraud. Following an investigation, the ICO found that – because of the way that the pre-2002 register had been used – the website did not comply with the first principle of the Data Protection Act.

8.84 The issues arising from the development of such services go considerably wider, however, and can be expected to become increasingly challenging as more and more information enters the public domain in electronically accessible form. The growth in social networking sites exacerbates the situation. It can be anticipated that more and more information of a very personal nature will be widely available with minimum effort and with no or minimal controls. The current controversy about possible public disclosure of MPs' home addresses illustrates strength of feeling on this issue.

8.85 ***Recommendation 18***: **We recommend that the government should commission a specific enquiry into online services that aggregate personal information, considering their scope, their implications and their regulation.**

8.86 During the course of our review, we encountered calls for more targeted and more specific reform in this field. Focus here was on access to the electoral register. The Representation of the People Regulations (England and Wales) 2001 and the Representation of the People (Scotland) Regulations

2001 govern access to both the full and edited electoral registers. Following amendments to those regulations in 2002, two versions of the register were created: a full register and an edited register. The full register contains details of all registered electors and is available for inspection under supervision by members of the public. It may be supplied and sold to certain specific people and organisations – primarily political parties for electoral purposes, and credit reference agencies – subject to restrictions on its use. The main use of the full register is to show who can vote in elections and referendums. Credit reference agencies can use it, but only to check names and addresses when people apply for credit, and for other purposes specified in law. It can also be used for crime prevention and law enforcement by organisations such as the police and security services.

8.87 The edited register is available for sale to anyone for any purpose. Its main clients are direct marketing companies and companies compiling directories. Members of the public can choose to have their details omitted from the edited register by ticking a box on their electoral registration or annual canvass form. Currently around 40 per cent of those registered to vote across the UK opt out in this way. However, the language used on these forms can be confusing, and many people do not realise it is the edited register that is on public sale.

8.88 In any event, we feel that selling the edited register is an unsatisfactory way for local authorities to treat personal information. It sends a particularly poor message to the public that personal information collected for something as vital as participation in the democratic process can be sold to 'anyone for any purpose'. And there is a belief that the sale of the electoral register deters some people from registering at all. We are sympathetic to the strong arguments made by the Association of Electoral Administrators and the Electoral Commission that the primary purpose of the electoral register is for electoral purposes.

8.89 ***Recommendation 19***: **We therefore *recommend* that the Government removes the provision allowing the sale of the edited electoral register. The edited register would therefore no longer serve any purpose and so should be abolished. This would not affect the sale of the full register to political parties or to credit reference agencies**.

Acknowledgments

Completing the work of this review would not have been possible without the participation and collaboration of so many of our contributors. We are immensely grateful to all those who gave evidence to the review, whether through our written consultation exercise – the results of which were enormously helpful – or through the series of illuminating discussion workshops or other meetings. Throughout the process of gathering evidence and compiling the report, the help we have received from contributors has been invaluable. We extend our thanks to all of them.

We are grateful to Ian Gambles for facilitating the series of discussion workshops so effectively; and for his help in reviewing the evidence of our written consultation. Ian's work in editing the summary of responses was very much appreciated, in particular as it helps crystallise the strong evidential foundations upon which our report rests. We are also grateful to Jennifer Potter who helped with the editing of the final drafts of our report.

Onora O'Neill and Edward Walker-Arnott kindly read a working draft of this report and provided much wise advice and food for thought. We are extremely grateful to both of them.

We would like to acknowledge the support of the Wellcome Trust, which allowed Mark Walport the necessary time and support to undertake this review, and provided facilities for a number of the workshops. We also appreciate the contribution of the Information Commissioner's Office which has provided expert advice, notably through the part-time secondment of Iain Bourne to the secretariat, and which has had to share a significant amount of Richard Thomas's time with this review.

Last, and most importantly, we are extremely grateful to our secretariat, so ably led by Martyn Taylor. Martyn and his team, Iain Bourne, Matt Cook, Amrit Lotay and Craig Robb, have worked very effectively in sifting and analysing the wealth of evidence we collected; and have provided the much needed stability for the review around the pressures of our respective 'day jobs'. A very big Thank You.

It goes without saying that while we share the credit with those who have helped us so much throughout the review, we are fully accountable for the contents of this report and its recommendations.

Produced July 2008