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 ISBN 978-1-84099-204-5

Data Sharing Review

Richard Thomas and Mark Walport

Data Sharing Review Report

Annexes

11 July 2008

Contents

Annex A - Terms of reference for the review

Established by the Justice Secretary, 25 October 2008

The review will consider whether there should be any changes to the way the Data Protection Act 1998 operates in the UK and the options for implementing any such changes. It will include recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection. It will also make recommendations how data sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability. To inform its recommendations, the review panel will consult with:

a. the devolved administrations

b. the European Commission

c. the academic and legal community and the media

d. representatives of the IT community and the private sector

e. a representative sample of government departments and agencies with an interest in data sharing and privacy

f. other parties identified by the review team

The recommendations will seek to take account of technological advances and strike a balance that ensures appropriate privacy and other safeguards for individuals and society, while enabling sharing information to protect the public, increasing transparency, enhancing public service delivery as well as the need to minimise the burden on business.

Annex B - Contributors to the review

The following individuals and organisations all made contributions to the Data Sharing Review.

A J Burnet
Acxiom Limited
Advisory Panel On Public Sector Information
Agencia Consulting Ltd
AHRC Research Centre for Studies in Intellectual Property and Technology Law
Alain Brun, European Commission
Alan Ferries
Allan Jackson
Andrew Evans
APACS
Archi Hipkins
Arthur Butterfield
Association of British Insurers
Association of Chief Police Officers of England, Wales & Northern Ireland
Association of Electoral Administrators
Association of Private Client Investment Managers & Stockbrokers
Association of the British Pharmaceutical Industry
Audit Commission
Barclays
Barnsley Metropolitan Borough Council
Barry Tighe
Basingstoke and Deane Borough Council & Hart District Council
Boots
Borders and Immigration Agency
Bristol Wessex Billing Services
British Airways
British Bankers Association
British Computer Society
British Humanist Association
British Insurance Brokers' Association
British Medical Association
British Sky Broadcasting
British Society for Human Genetics and Joint Committee on Medical Genetics
BT Group
Cabinet Office

Callcredit Limited
Camerawatch
Cancer Research UK
Capital One Bank (Europe)
Carol Hunt
CBPL/CPVP - Office of the Belgian Information Commissioner
Central Office of Information
Central Sponsor for Information Assurance
Centrica plc
Chaplaincy Academic and Accreditation Board
Charles Farrier
Cheshire Fire and Rescue Service
Chief Information Officers Council
Children's Rights Alliance for England
Chris Boxall
Chris Wilson
CIFAS
Confederation of British Industry
Connexions Cornwall and Devon
ContactPoint
Cornwall County Council
Council for Science and Technology
Crown Prosecution Service
Data Protection Forum
David Chisholm
David Edwards
Demos
Department for Children, Schools and Families
Department for Communities and Local Government
Department for Transport
Department for Work and Pensions
Department of Health
Direct Marketing Association
Don Bacon
Donald Ashton
DQM Group
Dr C.N.M Pounder
Dr Foster
Dr. Steven Van de Walle
Economic and Social Research Council

Edentity
Education Leeds
Education Otherwise
Electoral Commission
Elizabeth Bertoya
EnCoRe
Environment Agency
Equifax
Ernst & Young LLP
EURIM
Experian
Faculty of Public Health
Finance & Leasing Association
Financial Information Markets
Financial Services Authority
Foreign and Commonwealth Office
Foundation for Information Policy Research
Gambling Commission
GB Group
GE Money
General Medical Council
General Motors Europe
General Practice Research Database
GeneWatch UK
GlaxoSmithKline
Google
Government Social Research Unit
Her Majesty's Revenue and Customs
Home Office
HPI Limited
Human Genetics Commission
Identity and Passport Service
Information Commissioner's Office
Information Commissioner's Office (Wales)
InMezzo
Intellect
ITN
J N Payne
James Camp
John Shale

Kent Connects Partnership
Kevin Victor
Knowledge Council
Leeds City Council
Legal Complaints Service
Leicester City Council
Leicestershire Information Management Advisory Group
Lloyds TSB
LMG/Nectar
Local Authorities Coordinators of Regulatory Services
Local Government Association
Logicterm
London Borough of Brent
London Borough of Lambeth
London Councils
Low Incomes Tax Reform Group
MacRoberts
Market Research Society
Medical Research Council
Ministry of Defence
Ministry of Justice
National Association of Data Protection Officers
National Audit Office
National Cancer Research Institute (NCRI)
National Consumer Council
National Information Governance Board for Health and Social Care
National Offender Management Service
National Patient Safety Agency
National Police Improvement Agency
National Society for the Prevention of Cruelty to Children
Neal Hunt
Newspaper Publishers Association
Newspaper Society
NHS Confederation
NHS Grampian
NHS National Services Scotland
No2ID
North Yorkshire County Council
Northgate Public Services
Nottingham Trent University

Novartis
Nuffield Council on Bioethics
Office for National Statistics
Office of the Northern Ireland Civil Service
Office of the Secretariat & Legal Counsel International Pharmaceutical Privacy Consortium
Oxfordshire County Council
Patient Information Advisory Group
Penny Cooper
Periodical Publishers Association
Peter Hustinx, EU Data Protection Supervisor
Pfizer
PHG Foundation
Phorm UK
Privacy Group Ltd
Privacy Law and Business
Probation Service
Professor Alex Markham
Professor Brian Collins
Professor Charles Raab
Professor Gus Hosein
Professor Martin Bobrow
Professor Paul Boyle
Professor Ross Anderson
Professor Sally C Davies
Professor Simon Davies
Quicksilva Consultancy Services
R A Collinge
Reading Borough Council
Reed Elsevier
Registrar General for Scotland
Research Councils UK
Research In Motion
Research Information Network
Richard Paul-Jones
Rob Findlay
Roger Borthwick
Rosemary Jay
Royal Academy of Engineering
Royal Bank of Scotland

Royal College of General Practitioners
Royal College of Pathologists
Royal College of Physicians
Royal Pharmaceutical Society of Great Britain
Sapior Ltd
Scottish Ambulance Service
Scottish Daily Newspaper Society
Scottish Government
Serious Organised Crime Agency
Shirley Ann Judges
Sir David Varney
Sir Ian Magee
Society for Computers and Law
Society of Editors
South Hams District Council
Southwark Council
Statistics User Forum
Symantec
Telecommunications UK Fraud Forum Ltd
Tell Us Once
Tesco
The Academy of Medical Sciences
The BioIndustry Association
The Customer's Voice
The Institution of Engineering and Technology
The National Archives
The National Council for Voluntary Organisations
The Newspaper Society
The Open Rights Group
The REaD Group (UK) Ltd
The Times Newspaper Ltd
The Wellcome Trust
Tim Bull
UK Clinical Research Collaboration
UK Council of Caldicott Guardians
University of Dundee
Welsh Assembly Government
Wick Hill plc
Wirral Council
Yahoo

Annex C - Summaries of consultation responses

Introduction

1. The Data Sharing Review carried out a public consultation exercise on the use and sharing of personal information in the public and private sectors. The consultation period ran from 12 December 2007 to 15 February 2008. The consultation document is available online at: http://www.justice.gov.uk/docs/data-sharing-review-consultation-paper.pdf.

2. We received 214 responses, of which some 60 submissions came from private individuals, with the remainder coming from institutions. The responses were of considerable value to the work of the review and we are extremely grateful to all those who took the time to contribute in this way. Responses that we have permission to publish are available on our website, alongside our final report.

3. Given the large number of responses we received, we thought it would be useful to provide this summary of the main issues raised.

Section 1: Background

4. Respondents were asked to explain their own interest and involvement in information sharing.

5. *Individuals.* Some individuals responded in a professional capacity, but a significant number responded in order to raise their personal concerns around data sharing and to express their frustration with the way they felt Government handles their personal information. In particular, there was opposition to the proposed national identity register and identity cards. Several individuals called for a renewed and increased focus on privacy and liberty, which were considered quintessentially British qualities and essential for the health of a liberal and democratic society.

6. A recurring theme among members of the public was the disparity in power between the citizen and the state in relation to data sharing. It was said that the citizen has no choice but to use public (or publicly administrated) services, but equally had no choice or say over how their personal information is used once it was in the public sector. Whereas you could choose which private sector services you used, there was only one tax office, one benefits office and, for the majority of people, one NHS.

7. *Organisations.* A wide range of organisations responded, including central government departments, the devolved administrations, local authorities, private companies, representative bodies and pressure groups. For example, in the public sector the Department for Work and Pensions noted that it is one of the largest data custodians in Europe, responsible for approximately 73 million customer records, while many in local government highlighted the increasing trend towards local area partnership working, which necessitates information sharing in the fields of health, social care, education, and crime/community safety.

8. The representational and lobby groups who responded tended to focus on the importance of privacy and the need for safeguards to prevent undue interference with privacy. They illustrated this with the examples of healthcare and medical services, where highly personal information is often of necessity routinely collected, and financial services, where data breaches can leave individuals open to fraud on a massive scale.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

9. Section 2 of our consultation paper covered a very large amount of ground and elicited some particularly valuable responses. Here we summarise what was said about:

- Benefits
- Risks
- Excessive data collection
- Missed opportunities

10. Consultation responses showed a clear spectrum of opinions, with a significant minority at the opposing ends of the spectrum. However, there were relatively few respondents who saw data sharing as either intrinsically good or bad. Most respondents could appreciate the benefits that information sharing can bring, but recognised that the risks involved must be managed effectively.

Benefits

11. Various respondents described the general benefits associated with information sharing. These included:

- planning and delivering **faster, cheaper and more effective services** that can be tailored to customers' needs. This could lead to lower taxation and lower prices, because goods and services could become cheaper to provide;
- more effective **prevention and detection of crime**, including fraud, and improved public and community safety. There were, for example, numerous mentions of the information-sharing problems found after the enquiries into the Soham and Victoria Climbié murder cases; and
- more **convenience for citizens** and organisations, by avoiding the need to duplicate data collection exercises.

> "The exchange of personal information is necessary for the creation and delivery of almost all goods and services. Commerce could not exist without the exchange of personal information".
>
> **Symantec Inc.**

12. In addition to these commonly recurring themes, there were a great many sector-specific examples. Right across the medical/healthcare sector, for instance, there was a clear view that major benefits could be obtained from the sharing of personal information. Indeed, the overwhelming view of healthcare providers was that sharing personal health information was of great importance in ensuring patients received the safest, most effective and timely care possible. Efficient referrals from GPs to specialists and from specialists to wider care teams were said to help ensure patients' health problems were

dealt with at the earliest possible stage and in the best possible way. Important in this was the need for the care teams to be aware of the patients' past medical history so as to avoid incorrect diagnoses or repetitive testing. Moreover, in times of crisis, speedy information sharing could prove vital to a patient's survival chances (for example following a serious accident), as could immediate notification of the availability of a suitable organ for transplant.

13. Respondents in healthcare also emphasised the importance of data sharing in medical research. Such research benefits both individuals and society as a whole, and these benefits were listed as including improved understanding of the causes and patterns of disease in populations; stronger evidence about the effectiveness of treatments and preventive measures; and greater and more accurate surveillance of adverse effects. Several respondents referred to cancer research. Here, sharing personal information can allowing linkage of information across different fields of research, increasing the understanding of the factors that contribute to cancer development. It can prevent duplication of research effort, foster better collaboration between doctors, nurses and researchers. It can enrich research databases by bringing information from different sources together for analysis. Many of these benefits were recognised as being relevant to research more widely, not only to medical research.

> "Data sharing:
>
> - Facilitates high-quality, policy-relevant research by sharing and then combining datasets from different departments and agencies to form a full picture rather than analysing separate pieces of a jigsaw.
> - Reinforces open scientific inquiry thereby improving methods of data collection and measurements through the scrutiny of others.
> - Promotes new research and allows for the testing of new or alternative methods.
> - Reduces costs by avoiding duplicate data collection efforts.
> - Allows the creation of new datasets through the merging or linkage of two or more existing sources of information.
> - Provides an important resource for training in research by enabling new researchers to utilise existing data.
> - Can reduce the burden on respondents caused by multiple data collection efforts.
> - Reduces the information security risks associated with maintaining duplicated datasets in more than one location."
>
> **Economic and Social Research Council**

14. Private sector respondents offered numerous examples of the benefits that sharing personal information can bring. One example concerned the credit system, which could not function without the secure exchange of information between credit grantors and credit reference agencies, for example when someone applies for a mortgage. Other companies and firms suggested that information sharing allows marketing materials to be targeted at the appropriate consumers, making the marketing more effective and reducing environmental waste. Other private sector respondents said that information

sharing allows better market analysis, facilitates innovation and opens up markets for new goods and services.

15. Public sector respondents also recognised the importance of information sharing for service delivery, especially in terms of overcoming organisational boundaries and allowing collaborative working. For example, the Ministry of Defence referred to the information it shares to track, analyse and understand the effects of depleted uranium exposure on its personnel. HM Revenue & Customs described the way it shares information with the Department for Work and Pensions to ensure individuals receive the benefits they are entitled to. Departments and agencies such as the Ministry of Justice, Crown Prosecution Service and the Serious Organised Crime Agency explained how information sharing is used to prevent crime. The issues surrounding information sharing were perhaps illustrated best in the context of public protection and safety, where information sharing can, literally, be a matter of life or death. As one respondent remarked: "*In health and social care settings people do not die from breaches of confidentiality but do die from not sharing important information*".

16. A recurring message, particularly from respondents from the public sector, was that citizens expect organisations to share information about them where this is necessary to provide services.

> "The sharing of information about individuals between departments of the same authority - and increasingly between public agencies operating within an area - helps deliver joined up services to those individuals. For example, a vulnerable elderly person can benefit where the council's adult social care service shares information with the local health service; a young person's preparation for employment may be facilitated if their school liaises with the local Learning and Skills Council to produce a rounded profile of attainment and training requirements; the sharing of information amongst police, social care and school can help protect a vulnerable child; and a young person leaving care will benefit from information sharing between the county council that is responsible for care and the district council that is responsible for housing. **Government and citizen alike expect effective liaison of this sort to happen**. Local Area Agreements depend on joint planning, service delivery and performance management by public sector organisations working together. This work is underpinned by a shared view of local people and their needs".
>
> **Local Government Association**

17. A minority of respondents were sceptical about these benefits, and argued for alternative, privacy enhancing approaches to sharing information in a personally identifiable form. Some argued that a more 'user centric' approach to identity management is needed, for example by allowing people to hold their own information on an encrypted electronic card. Individuals would then have far more control over who has, or has not, got access to information about them. Some argued that current information sharing models are too organisation-centric and do not give due weight to the needs of individuals and their desire for control over information about them.

18. While most respondents accepted the desirability of sharing personal information in certain contexts, many acknowledged that benefits could not be considered in isolation. As Professors 6, Raab and Bellamy put it: "s*imply enumerating benefits does not obviate the need for agencies to specify the circumstances in which they are likely to be*

relevant". They added that: *"[a]gencies should not only be aware of [possible] benefits and disbenefits, but should assess their scale and probability, and also assess the scale and probability of the risks that they are prepared to accept in their pursuit*".

Risks

19. Respondents across the board provided a fairly consistent account of the dangers and risks associated with information sharing. Many referred to the risk of personal information being lost, stolen or abused when sharing takes place, resulting in anything from inconvenience or embarrassment to financial or reputational damage, or in extreme cases to mental health problems or even suicide.

> "Of prime concern to individuals is the loss of control and intrusion into their private lives resulting from a lack of privacy. Other concerns include the mishandling of information that can lead to identity theft, and the dissemination of inaccurate information that can result in social stigma or loss of credit."
>
> "Without adequate protections, both public and private sector plans to use personal information, including e-government and e-commerce can be undermined by lack of public trust and consumer confidence."
>
> **The National Consumer Council**

20. In their submission, Professors 6, Raab and Bellamy identified four categories of risk, which corresponded fairly well with the majority of evidence received. The four categories were:

    i) **indignity** - unnecessary exposure of facts/suspicions, for example disclosure to an agency not concerned with gynaecological matters of the fact that a woman client may have had a termination;

    ii) **injustice** - stigmatisation resulting from wrongly disclosed information, leading to loss or denial of, for example, employment, training, or credit;

    iii) **inappropriate treatment** - unwarranted interventions by agencies into the lives of individuals or their families, for example with draconian action being taken by mental health or child protection workers based on misinterpreted/uncontextualised data; and

    iv) **ineffective service delivery** - because, for example, individuals do not trust agencies sufficiently to provide full and accurate information as required.

21. Most respondents focused on two main areas of risk. The first involved **trust**: examples of data breaches were becoming so common that the public may be losing faith in the ability of organisations to protect personal information properly. This could lead to individuals not co-operating with service providers, for example by refusing to provide information, or by providing inaccurate or incomplete information. This argument was advanced with particular conviction by respondents from the medical and healthcare sector, where there was almost unanimous concern there that data losses, breaches of confidentiality, or failures to respect individuals' wishes could lead to a loss of trust in doctors, resulting in patients being reluctant to provide necessary information to their GPs, to the detriment of themselves and the public.

22. The second main issue that respondents focused on concerned the accuracy of information and the context in which it is held. There was a concern that once inaccurate information is shared, it can be difficult to get it corrected. There was also concern that data items could be viewed without the necessary contextual backdrop, leading to flawed decisions being made, causing harm to individuals or lost opportunities for social benefits. An example given was that of the UK's National Insurance numbers, an important identifier for various official purposes. The country has a population of around 60 million, but there are around 80 million active NI numbers. This suggests that some individuals have several numbers, meaning there may be several different records about the same person. Many respondents pointed out the importance of context, notably in relation to information obtained through Criminal Reference Bureau (CRB) checks. Denial of employment to an individual on the basis of a single item of data - that they have a criminal record - without access to or understanding of the context of that data, can lead to harm just as failure to share that data at all can lead to harm of a different kind.

> "There is a risk that individuals or groups might be prejudiced if personal information is shared and there is a lack of contextual understanding about how and for what purpose information was originally collected for and how it will be used. There were reports in autumn 2007 of individuals who had been refused employment because they had a criminal record, on further investigation it transpired that they were for minor offences committed 20 years previously".
>
> **Leicester Information Management Advisory Group**

23. Many respondents suggested that when data is shared, the risks to individuals are increased. The more widely personal information is shared, the more likely it is that a breach of confidentiality could occur, for example where anonymised data sets are brought together, allowing an individual to be 're-identified'. It was also suggested that when information is shared, there is a greater risk of it being lost accidentally or being misused deliberately.

> "There is an inherent security risk every time personal information is shared between organisations."
>
> **Information Commissioner's Office**

24. Linked with this point, some respondents noted that there are few, if any, technical controls capable of protecting personal information once it has been disclosed to another organisation. An organisation may be able to respect the data subject's wishes, for example limits on disclosure or use, when the information is in its own possession. However, there is a risk that this will break down once the information is disclosed to another organisation. It could also be difficult, or impossible, for individuals to challenge the way the other organisation is handling their personal information. There was also a suspicion that datasets are being combined and analysed without there being a clear rationale for doing this.

25. A message that came through with resounding clarity from members of the public was that there were significant concerns over the way in which the State uses the personal information of its citizens. Phrases like "*Government incompetence*", "*database state*", "*surveillance society*" and even "*totalitarian state*" were found in a number of

submissions. Whilst the sample was relatively small and not necessarily a representative cross-section, this view is illustrative of wider concerns evidenced in, for example, opinion poll findings. The most common complaint from our non-organisational respondents about the Government's handling of personal information concerned the sale of vehicle registration details by the DVLA to private car parking/clamping operators. One respondent included details of a case where a car had been crushed, having been identified mistakenly as untaxed and uninsured.

26. It was not only individual members of the public that raised such concerns. Several organisations, typically those with a wider interest in data protection policy, advanced similar arguments. For example, organisations working in the field of criminal justice identified the risk of vigilantism if information about offenders or suspects were to be leaked or lost. Some respondents pointed to real life examples where entirely innocent people had been singled out on the basis of inaccurate, incomplete or misinterpreted information.

> "By sharing personal information we surrender control in the longer term by leaving ourselves open to judgement by different groups in different ways. The drive to personalise or tailor services, which is shaped by those judgements, can lead to differences between what people experience and have access to. This can mean a narrowing of experience, can lead to social exclusion, and has significant implications for how we live together as a society"
>
> **Demos**

27. Some contributors, including children's rights groups, focused on recent Government initiatives like ContactPoint and the Common Assessment Framework, saying that they posed an unacceptable risk to young people. Other groups cited with approval Parliament's Joint Committee on Human Rights' Nineteenth Report (September 2004), which said that *"if the justification for information sharing about children is that it is always proportionate where the purpose is to identify children who need child welfare services, there is no meaningful content left to a child's Article 8 right to privacy and confidentiality in their personal information"*. However, other respondents felt that ContactPoint presented opportunities in child protection and explained that although there were security concerns, these had been thought through properly as the initiative developed.

28. The Association of Electoral Administrators, among others, suggested that the use of information from the Electoral Register for purposes other than electoral administration (by, for example, direct marketing companies) risks discouraging electors from registering to vote.

29. Overall, while some respondents felt that the benefits of data sharing within public services were sometimes oversold, and that there was a risk in overemphasising the ability to deliver social justice through the use and sharing of personal information, the majority considered that the best approach was to put in place effective risk management strategies, helping to minimise the prospect of harm but delivering the benefits that information sharing can bring. The majority view was that as a general rule the risks of *not* sharing information outweighed the risks of sharing.

Excessive data collection

30. We asked for examples of cases where respondents thought excessive personal information was being collected. A large number of respondents, members of the public and organisations, felt that the Government - both central and local - held too much information, and was allowing too many people access it. They also suspected that a large amount of information was being transferred between organisations when a lesser amount would suffice. The example frequently cited was last November's HM Revenue & Customs data breach involving the missing data disks. Very few, if any, respondents thought it inappropriate for the National Audit Office to have access to HMRC data, but there was concern that HMRC apparently provided irrelevant and unnecessary data to the NAO. The widely held view was that personal information should only be held and shared where it is strictly necessary.

> "It is not, perhaps, a question of whether public authorities hold too much personal information, but rather that too much information is available to too many people, e.g. departments or offices that have access to information they do not need"
>
> **Intellect**

31. The practice of collecting and storing the same information in a number of different databases across public sector organisations was pointed to as unnecessary data duplication, which in itself increased the risk of data breaches. Large databases, such as the national identity register, ContactPoint, Connecting for Health, and the Police National Computer, were mentioned repeatedly in the context of excessive or disproportionate data collection. Many respondents raised concerns about the National DNA Database, suggesting that collecting DNA from people who had not been convicted of any criminal offence was not acceptable.

> "The Oyster Card, Transport for London (TfL)'s electronic ticketing system, retains centralised logs of individuals' journey details on an eight-week rolling basis before anonymising the data and retaining it for research purposes. Such data have never been collected before, and have the potential to present a detailed picture of an individual's life. The merits of storing such data centrally are not immediately clear from the perspective of functionality. It is therefore unclear why this feature was built into the system."
>
> **Open Rights Group**

32. Respondents also raised some concerns about the use of personal information in the private sector. Some suggested that banks held too much personal information and sent too much of it through the post. Others thought mobile phone companies and supermarkets collected too much information. Another example cited was the hospitality industry, where it was felt that hotels sometimes demanded too much personal identifying information from guests at check-in. Some respondents were concerned that the merger of technology companies could lead to the creation of massive data sets about individuals' use of the internet. Others complained about the amount of junk mail they receive, seeing this as evidence of information about them being shared too widely.

Missed opportunities

> "We have always found a basis for sharing personal information where it is considered necessary for us to do so for the exercise of our functions. However, where the purpose of the data sharing is to enable another public authority (e.g. HMRC or DWP) to fulfil its functions, then we frequently face the issue of whether or not we have the vires to share the information. Therefore, it might be helpful to consider the appropriateness of bringing forward legislation to confer upon public authorities generally a vires to share personal data where it is in the public interest to do so."
>
> **Welsh Executive Government**

33. The clear message from this part of the consultation was that there is extensive and widespread confusion over what the law says, what it permits and what it prevents. This confusion often frustrates beneficial data sharing, either thwarting it entirely or making it more difficult.

34. Moreover, some respondents commented that "*lurid tabloid stories*" do nothing to further public understanding of data management rules, and in fact contribute to a risk-averse culture. More responsible, factual and positive reporting and presentation would help to guard against this.

35. Concerns about a lack of legal clarity came from both the public and private sectors, but seemed to be a particular issue for local authorities. Local authorities are increasingly being asked to work together, but a number of them said a lack of common understanding of the law has become a real problem. Various respondents commented that, although all local authorities are supposedly "in the same game", each one tends to "play by different rules", with one Council in England saying that each of the 433 local authorities across the country have "different interpretations of what information can be shared and with whom". A particular example quoted in responses was that sharing between the two tiers of local government in the same area is often prevented, meaning that residents have to provide the same information to two separate bodies, which is inconvenient for the individuals concerned, and costly for the authorities.

> "Responses from some local authorities to EURIM questioning indicate that the DPA is perceived to be a barrier even when it is recognised in reality not to be; others clearly believe that the DPA is in reality a barrier, citing the Childrens Act as one example where the law is contradictory. Clarity and advice from the ICO was also perceived to be lacking by some."
>
> **EURIM**

36. We received several examples of situations where fear over the application of data protection law, or the law itself, prevented beneficial information sharing. For example, it was commented that in Scotland anonymised population census and hospital discharge information was shared to aid understanding of social determinants for health, but that this was not done in England. This could have many benefits and could aid social marketing for public health improvement. One respondent highlighted a campaign it carried out for a government department, where the department was trying to contact certain people who had been on long term sick leave. The department in question held information about those individuals, but declined to release it. Therefore the respondent organisation had to resort to

field marketing and putting posters in GP surgeries, entailing a lot of unnecessary waste, and meaning that not all the relevant individuals were made aware of the campaign.

37. The Office for National Statistics (ONS) gave two case studies, which it suggested illustrated how greater data sharing could be advantageous:

- ***population and migration statistics*** - population statistics are used to allocate resources, support policy development and review, plan and deliver services, for example in the areas of health, education and housing. According to the ONS, there is currently no single source of data that can be used to measure migration flows or monitor pattern changes. The Statistics Commission has estimated that around £1bn might be misallocated due to inadequate statistics. Bringing together the different sources would mean the possibility of building a more complete statistical picture and forming an authoritative basis on which to plan; and

- ***economic and business statistics*** - the Government requires comprehensive, accurate and timely information to manage the economy; to encourage enterprise and innovation; and to understand the nature and impact of structural and other changes. Access to a range of administrative sources, including data collected by HM Revenue & Customs and the Department for Work & Pensions would improve both national and regional statistics, reduce the burden on data suppliers (most notably small businesses), and generate significant costs savings. In particular, the availability of tax data for individual businesses would enable ONS to improve efficiency and value for money in its data collection and increase quality by extending coverage to small businesses.

38. In the private sector, respondents from the financial services sector cited situations where advantageous sharing - for fraud prevention and responsible lending purposes, for example - was not taking place, often because of confusion around the legal position. A number of respondents touched on the topical issue of utility companies sharing personal information with public sector organisations involved in, for example, protection of the elderly. This type of information exchange could allow a social services department to intervene where a vulnerable person is about to be cut-off for non-payment of a utility bill.

> "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**

Section 3: The legal framework

39. The questions in section 3 of our consultation paper sought views on the strengths and weakness of the Data Protection Act, including a focus on the Act's principles and any barriers there might be to the Act working effectively; on the wider legal landscape, including the interplay between the Data Protection Act and other domestic and European law; and on the data protection enforcement regime and the powers and sanctions available under it.

The Data Protection Act

40. There was a strong consensus that the Data Protection Act (the Act) generally works well and that its principles are basically sound. In particular, respondents recognised the Act's transparency provisions and the rights it gives to individuals, e.g. the right to access personal information and to have inaccurate information corrected. Some thought that the Act was a particularly important defence for individuals facing requests under Freedom of Information law for access to information about them. However, there were very few unqualified supporters of the Act. Most thought the Act was only "*moderately* successful" or was working "*reasonably* well". Many respondents supported the principles and purpose of the Act, but thought it was too complex and often misunderstood. The drafting of the Act was thought to be too technical - "*written by lawyers for lawyers*" - but one respondent thought that even lawyers find it hard to understand. There was a strong feeling that the words of the law are very hard to apply in practice.

> "There are many myths surrounding the DPA - it appears to be one of the most frequently cited yet least understood pieces of legislation."
>
> **The National Archive**

41. Some of the Act's terminology was singled out as a particular source of confusion. This included:

- "consent"
- "crime and disorder"
- "data controller"
- "data processor"
- "fair"
- "identifiable"
- "legitimate interest"
- "necessary"
- "personal data"
- "prejudice"
- "public protection"
- "reasonable"
- "relevant filing system"
- "sensitive personal data"
- "specified and lawful purpose"

> "In theory, the DPA provides a powerful and flexible framework for data processing: it sets out a list of data processing principles and provides for a framework of checks and balances. In practice however, some of the principles are unclear (such as the obligation for fair and lawful processing) and the legislation is unduly complex."
>
> **The PHG Foundation**

42. While the Act creates wide areas for discretionary decision-making, frontline staff frequently want legislation to offer them "algorithms" that would obviate the need for

judgment. Thus where organisations are not clear about what the law means in practice, their default position is to adopt an overly "restrictive", "conservative" or "risk averse" approach, meaning that sharing does not take place when it could (or should) do and that potential benefits are not being realised.

> "The simplicity and elegance of the data protection principles is diminished by the number and complexity of the exceptions, some of which are described in the Annexes to the DPA, while others are scattered around in other bits of legislation. A single piece of legislation, which deals with data-protection and data-sharing subjects in an elegant and comprehensive way, would be a great help"
>
> **Edentity Limited**

43. A number of respondents made specific suggestions about the workings of the legislation. Among the issues raised were:

- the **notification procedure** should be reviewed. Many respondents said that, although registering the names and addresses of data controllers could be useful, the registration of rather vague 'purposes' is relatively meaningless. If the need for notification remained, then data controllers should be required to say which organisations they share information with and to be more specific about their reasons for doing this;

- the data protection laws should extend to **deceased people**, particularly where the death happened relatively recently and the data involved is sensitive health information, which could presumably have genetic implications and therefore potentially put at risk the privacy of surviving relatives;

- there is a lack of clarity around **responsibility and accountability**, particularly where two or more data controllers hold the same information. This "controllers in common" scenario was picked up on by several respondents, who each called for more precision in terms of where accountability lies;

- the Act is not specific enough in enabling correctly governed **research**. In particular, the Act should include a power to enable anonymisation and pseudonymisation and should explicitly mention systems of "trusted third parties" (i.e. where the use of personal information by an organisation can be minimised by ensuring all identifiable data is controlled securely by a licensed body at arms length, so only allowing completely anonymised versions of it to be used by the organisation itself);

- the **subject access** system, although generally seen as a positive aspect of the regulatory regime (see further comments in section 4), was also seen by some as imposing disproportionate burdens, and it was argued that the Act should have better provisions for rejecting vexatious or otherwise inappropriate requests, perhaps mirroring those in the Freedom of Information Act.

The second principle

> "The second principle… is a constant reminder that data controllers manage that information on behalf of the data subjects rather than 'owning' the data"
>
> **The Gambling Commission**

44. Overall, the Act's eight principles, listed at the end of its first schedule and which set out the broad philosophy underlying the entirety of the Act's framework, were thought by respondents to be useful. Because of its obvious resonance with the sharing of personal information, our consultation document focused in particular on the Act's second principle, which reads

    Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. (Data Protection Act 1998, c29, Schedule 1, Part I, para 2)

45. The second principle was seen by the majority of respondents as being a valuable protection against the abuse of personal information, because it links the subsequent use with the initial collection of information. So, in effect, the principle acts a mechanism to prevent individuals being surprised, some way down the line, that their information has been reused in a way they would clearly not have expected. However, some respondents thought that the meaning of the second principle is unclear, and that it can seem too flexible or too inflexible, depending on the circumstances. The effect of the second principle also depends on how narrowly or broadly the organisation initially specifies its purposes. So for example, where collecting personal information expressly for the purpose of "service development" or "marketing", an organisation would find it relatively easy to justify all subsequent intended uses within the bounds of the second principle.

> "Without a categorisation which is generally agreed, "compatible with" can be interpreted loosely enough that almost any purpose could be instantiated even though it was not the one for which the data was originally collected"
>
> **Professor Brian Collins**

46. A particular concern of some respondents was with public sector organisations' compliance with the second principle. There was a perception that Government could and did legislate around the second principle by creating statutory gateways, giving authority to schemes that would on the face of it be prevented by the second principle.

Interplay with other law

47. Respondents tended to see the relationship between the Data Protection Act and other elements of the law as being particularly confusing. In particular, respondents were confused by the interplay between the Act, the common law of confidentiality, other UK legislation and the European Directive. In terms of particular statutes, the Human Rights Act and Freedom of Information Act were most often quoted, but mention was also made of the Finance Act 1989, the Crime & Disorder Act 1998, section 115, the Children Act 2004, and the Housing Act. The large number of statutory gateways, which provide the legal authority to share information in specific instances, were criticised as being widely dispersed in unconnected pieces of legislation, leading to an overall picture which was both opaque and confusing.

48. A number of respondents argued that there is a need for a new legal framework specifically for information sharing. Others called for a general public sector power to share, or for sector-specific regulation, for example a power to share for child protection purposes.

Powers and sanctions

49. A large number of comments focused on the inadequacy of the powers and sanctions available to the Information Commissioner.

> "even if the Act was simple to understand and apply, it can appear that there is little reason for some data controllers to comply with the Act as in practice a failure to comply is rarely met with a significant consequence"
>
> **Data Protection Forum**

50. The evidence we received pre-dated the Criminal Justice and Immigration Act 2008, and the amendments made under that legislation to the Data Protection Act. The DPA's new section 55A, which was inserted by section 144 of the 2008 Act, will (once it is brought into effect) provide the Information Commissioner with the power to fine those adjudged to have deliberately or recklessly committed serious breaches of the Act and its principles. The provision will strengthen the regulatory powers available to the Commissioner.

51. Many respondents said that they would like to see even greater changes. Members of the public, in particular, thought the ICO "a toothless tiger", and the majority view among both individuals and organisations was that the Data Protection Act should include stronger penalties and sanctions, and that the Information Commissioner should be given increased powers and resources to carry out his duties more effectively. There was wide support for the Information Commissioner to have the powers to carry out unannounced audits and inspections. Numerous respondents commented that Information Commissioner's powers should be more akin to those of the Financial Services Authority (FSA) or the Health and Safety Executive (HSE), and some even argued that the courts should be able to impose custodial sentences for gross mismanagement or deliberate misuse of information.

> "We believe it is appropriate for the Information Commissioner's Office to demand powers similar to those of the Health and Safety Executive. The Data Protection Act will not be taken seriously in businesses at Board Level until this happens."
>
> **Open Rights Group**

52. The analogy between the ICO and the FSA was drawn by many, including representatives of the financial sector. The FSA can levy very large fines on financial services providers found to be handling the information they are responsible for carelessly, but the Information Commissioner cannot currently do so. Some respondents suggested that the ICO's powers are so weak that the cost of putting proper information management systems in place would be greater than the likely cost of any regulatory action that could be taken against them, particularly as the chances of being caught out are minimal so long as the Commissioner's powers of inspection are as restricted as they currently are. This, respondents suggested, was a disincentive to putting effective

information management processes in place. Many of them, including the FSA itself, thought it unfair that under the current regime financial services firms can be penalised for their errors, but other organisations, which may handle huge quantities of personal information, fall outside the regulatory regime.

> "the sanctions and powers of the FSA exceed those of non-financial services regulators, including 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 FSA's rules or principles have been breached… We would strongly support a change in legislation which would give the ICO such powers".
>
> **Financial Services Authority**

53. The calls for additional powers were not unqualified. Some argued that any additional powers had to be proportionate and not unduly burdensome. Some also suggested that a few isolated instances of high-profile data breaches should not be allowed to lead to disproportionate amounts of additional red tape. But generally speaking, respondents could see the case for additional powers and resources for the Information Commissioner.

54. Part of the purpose of the additional resources respondents wanted to see available to the Commissioner was to enable him to offer better guidance and training, and develop a clearer, simpler framework for sharing personal information. Indeed there was a consensus amongst respondents that the ICO should strive to produce better guidance, especially in the context of an evolving legal framework, and should work with government and industry to develop better training for information practitioners.

> "If data sharing is to 'take root', then DPA will need to be amended or new enabling legislation introduced. These legislative changes would need to be supported by Codes of Practice and/or detailed guidance… Further and more stringent penalties may [also] be necessary to ensure that the attention of Data Controllers, and individuals who are accountable, is focussed firmly on the safeguarding of personal information."
>
> **Northern Ireland Civil Service**

Section 4: Consent and transparency

Consent

55. The issue of consent aroused a wide range of comment, and it was evident that there is much confusion over the extent and nature of the current requirement for consent, and much disagreement over what role consent should play in data sharing decisions.

> "There is a lack of clarity about what constitutes valid consent for data sharing, and how that consent should be managed. Current data collection mechanisms do not provide sufficient granularity for the individual to consent to what information is collected, how

> long it is held, with whom it is shared, and the purposes of sharing. Generalised 'opt-in / opt-out' notices do not cover a necessary level of detail, and rarely provide a transparent mechanism for data subjects to subsequently change their consent permissions or force the deletion of given personal data from its initial storage location and all other locations to which it has been transmitted for other purposes."
>
> **Privacy Enterprise Group**

56. A large number of respondents suggested that there was significant ambiguity around 'informed' consent, with concerns about whether consent could ever be truly informed, in particular when considering future uses or prospective consent. There was a view expressed by a range of respondents that consent was not given the respect that it deserved, with too many instances of organisations supposedly seeking the agreement of data subjects by burying provisions in lengthy and complicated terms and conditions, which by the obscure nature of the methods used could never constitute real agreement. Further, respondents highlighted cases where organisations claimed that they were seeking consent when in fact the use of personal information was a necessary part of the transaction and would be justified legally on other grounds even if consent were not provided. The very fact that consent was purportedly sought in those circumstances devalued it as a concept.

57. Issues of consent were particularly resonant in the healthcare and medical sector. Consent for secondary uses of health data was raised, with respondents calling for better guidance. In this context, some respondents supported the notion of "implied consent", arguing that when, for example, a patient takes advantage of healthcare services they should be deemed to have provided implicit consent for the use of their personal information in health research. However, there was also a recognition among some that patients could feel unfairly pressurised into giving consent for fear of receiving inferior treatment if they were to refuse. Similar arguments were advanced in relation to other sectors.

> "If consent was needed before sharing took place, sharing would never happen. There will always be people who refuse to share, putting personal interest above the well-being of society. The cost of separating out data covered by such refusals, linked with the costs or evidencing consent and maintaining it are enormous."
> **Leicester City Council**

58. In the field of medical research, two particular problem areas were identified. First, there was uncertainty over the need to obtain consent to access medical records to identify eligible research participants - in order to ask them for their consent to participate in research. We were told that this perceived requirement to obtain "consent to consent" causes enormous logistical problems for researchers and healthcare institutions and is having a negative impact on the ability to conduct large scale studies. Second, there is confusion about whether giving consent has to be a positive action, or whether a failure to opt out qualifies as valid consent for the purposes of the DPA.

59. The debate about whether the DPA required consent exposed a wider debate about how much control people should have over information about them, and whether, therefore, consent ought to be the primary precondition for sharing information. There were different views about this. Some felt it was highly undesirable to share any information

without the full and informed consent of the individual(s) concerned, others saw reliance on consent to be misconceived both in philosophical and practical terms. However, most respondents thought that consent was desirable in some circumstances, but impractical in others.

60. Many respondents started from the premise that consent is a valid way of legitimising the sharing of personal information. Consent should be sought where possible and appropriate, and where it is sought it should be genuine and informed. Whilst most respondents agreed with this, many recognised the limitations of permission-based sharing. Consent was clearly not valid in contexts such as crime prevention or public protection; or where mental capacity issues might be relevant; or where there are obvious benefits to society but where practical constraints make it very difficult to obtain all the permissions required. It was also recognised that in some cases consent could be overridden in the wider public interest, or where the law specifically provides for this.

61. No respondents thought that an entirely consent-based information system was feasible or desirable, and the majority view echoed that expressed by the AHRC Research Centre for Studies in Intellectual Property and Technology Law, University of Edinburgh, which submitted:

> *"the fetishisation of consent ... is an attitude prevalent among many regulators, including ethics committees, whereby the obtaining of consent has come to be seen as both necessary and sufficient to legitimate data handling and sharing when it is neither; nor, is it achievable or even desirable in some cases. This is not to belie the importance of informing individuals about data processing or the value of consent in appropriate circumstances, but it does suggest that more should be done to stress the important public interest which can be served by legitimate data sharing, especially in the context of robust scientific and medical research".*

Transparency

62. There was a far greater degree of consensus on the issue of transparency than there was on consent. There was a general and widespread acceptance that transparency was extremely desirable and that where possible it should be enhanced.

> "Transparency is a key requirement in this area and will increasingly become important to citizens. Citizens' concerns in this area could be reduced through greater clarity concerning what information is held about individuals by whom, with audit trails to provide greater transparency to the individual in tracing how their data is being used."
>
> **BT**

63. There was general consensus that far greater transparency was required in respect of the use of personal information and there was broad support for the Information Commissioner's Framework Code of Practice for Sharing Personal Information. Many advocated a more open approach to policy development and practice, suggesting that personal information compliance results should be published and that organisations should carry out and publish Privacy Impact Assessments (PIAs). PIAs would however have to be a genuine process, not a regulatory tick-box exercise. Further, organisations should be required to produce simple, understandable explanations of their policy and practices in relation to personal information, and some went on to suggest that 'data

management impact assessments' could be conducted by external agencies to ensure effective checks on privacy policies.

64. Many respondents argued that people should be able to find out more easily what data is being held about them, check the accuracy of such data, and get it changed promptly, across organisations, if it is inaccurate. Many suggested that the existing subject access requests regime needed to be reviewed and updated, to take advantage of new technologies. There were a number of calls for reducing the current 40-day deadline where the information is stored electronically and should be easy to retrieve. The charge for giving subject access was criticised, with many fearing that charging at all could act as a barrier to access, and therefore reduce overall transparency. Some respondents said that subject access should be free, because information technology makes it so much easier to retrieve and despatch information. Some respondents noted that HMRC already waives the standard £10 charge, proving that free access could be workable in practice. Others suggested that more should be done to make children's personal information available to them (the children). It was also suggested that individuals should be able to make a single request in order to receive information about them from a number of organisations, given that those organisations may be sharing information about the individual.

> "organisations should be clear about how data they collect will be used and shared. In particular, data protection notifications could be more specific so that the public can judge whether processing is legitimate."
>
> **Research Councils UK**

65. Those who wanted greater transparency called for a number of specific improvements, including:

- shorter, standardised Fair Processing Notices (FPNs) in plain English. A particular sector could agree a standard notice, which could be posted on the website of the relevant representative or trade association. This would allow the public to become more familiar with standard terms, and would allow them to recognise where any particular organisation departs from the sectoral standard;

- improvements to the present DPA notification system, which was widely seen as an administrative burden, but one which provides no real or significant benefit to the individual, organisation or regulator. If notification is to remain, some suggested that it should provide the ICO with substantive information as to how organisations process data, and be a starting point for any audit. There were also several mentions of the Freedom of Information Act publication schemes, which respondents thought could have beneficial effect in the data protection arena;

- 'track back' facilities, that would allow, for example, an individual who receives junk mail to trace where the direct marketing company obtained his/her data from should be considered;

- wider use of 'user-centric' ID management systems, giving individuals much more knowledge of, and control over, the use and sharing of their personal information; and

- systemic improvements to standards of guardianship, ownership, responsibility and accountability, with a particular emphasis on senior-level management of information security issues.

66. Organisations across the sectors should do more to explain what they are seeking to achieve by using or sharing people's information, and should provide clear and accessible information about what personal information they hold, why they hold it, how they use it, with whom they share it, and how long they retain it. It seemed to be generally felt that the public needs a much better explanation of what is happening to information about them, and that a number of methods need to be used to provide this.

> "Departments [must] communicate more with the public and explain why and how their personal information is to be handled and shared, especially in the light of the recent and various high profile losses of personal data. We would use public consultations as a principal means of communication, though greater use of websites and leaflets would also help us get our message across. The inclusion of material about information sharing in Departmental Publication Schemes would be another means of making more transparent our activities on this front."
>
> **Northern Ireland Civil Service**

67. A minority of respondents thought that existing transparency arrangements were good enough. Some argued that strengthening individuals' rights, allowing more access at lower cost would amount to an additional and disproportionate burden on organisations. The lack of any provision for protecting organisations against repeated or vexatious applications was again cited, as was a concern over the inability to recover the actual cost of providing subject access. It was also suggested that more transparency could result in weakened data security.

Section 5: Technology

68. This section of our consultation document focused on the impact that technology has had on the sharing of personal information. It asked questions about technological safeguards for protecting personal information and about the role of privacy enhancing techniques (PETs), such as anonymisation or pseudonymisation.

> "The entire question has developed because it has become practical to manage, exchange, match and mine vast quantities of information about people and their personal lives, rapidly and without their involvement. The technological capacity and the bureaucratic imperative to record and report that it facilitates have far outpaced social change. It is like the Black Death: the population has no natural resistance and no real understanding of what is happening and why."
>
> **No2ID**

69. Respondents agreed that advances in information technology pose risks and promise benefits. All respondents recognised that the growth in computing power has brought about the possibility of ever larger datasets that are subject to much more intensive, and potentially intrusive, analysis and exchange between organisations. Whereas once, files containing personal information enjoyed what one respondent described as "*privacy through obscurity living in dusty file cabinets*", today information can be moved at the

speed of light to the other side of the world and be duplicated and/or manipulated repeatedly at very little cost. This has obviously brought benefits, for example by greatly enhancing the ability of researchers to carry out effective analysis of large amounts of data brought together from a range of sources. However, some expressed a fear that sometimes things are being done simply because technology allows it, without adequate consideration of the social impact of technology.

70. Respondents also highlighted the security risks of holding large amounts of electronic personal information that can be shared, corrupted or lost almost instantaneously, or which can be compromised by a hacking or spy-ware attack. Portable devices pose particular security challenges, whilst large centralised databases were seen as inherently risky. It was suggested that the massive storage capacity of many computers means that more information is being collected and retained than is necessary, and that it is often not being kept up to date. Organisations which fail to take proper precautions when disposing of obsolete systems holding personal data, or which outsource their data handling or back-up operations to third parties can expose personal information to an increased risk of loss or misuse.

71. Respondents recognised that technology can be used to enhance security and privacy. However, many respondents suggested that technological focus has tended to be on delivery of functions and services, rather than on security and privacy.

> "whilst technologies for the protection of personal information are available, they do not provide the same business benefits and are not being used as widely"
>
> **Data Protection Forum**

72. Technological solutions were recognised as only being as strong as their weakest link, and almost invariably that weakest link was seen as being their human operators. It was suggested that there was too much corporate focus on technological development, and not enough on the training of staff or the implementation of the policies and procedures needed to deploy technology safely. Many respondents focused on the tendency of some, particularly in younger generations, to exchange information through social networking websites to a degree which risked compromising their own interests. Many found it hard to understand why the social network site generation might still be so unwilling to provide information about themselves in other contexts. Some doubt was expressed as to whether individuals have the *nous* to safeguard their own interests in the new electronic age. More public education and training was called for here.

73. Respondents recognised that 'off the shelf' security products were becoming increasingly available. Many respondents thought there ought to be mandated best practice standards for encrypting data. However, the general view was that whilst best practice should be observed, the pace of technological evolution means that any attempt to specify minimum standards in legislation would fail. It was generally felt that the law works best by setting out general principles in this area, leaving the definition of specific standards to the market, which is often led by professional institutions, industry-wide representative groups or sectoral regulators. In this vein, many also called for the removal of unnecessary domestic and international legal restrictions presently in place on the development and sale of software packages designed to help protect data.

> "there is an 'arms race' between those who seek to break encryption and those who seek to strengthen it. The former are greatly helped by Moore's Law (which predicts the doubling of processing power every two years), whereas the latter are hindered by export control laws"
>
> **Royal Academy of Engineers**

74. Many responses focused on the issue of using personal information for research, audit and statistical analysis. It seems that this is a particularly fertile area for the deployment of techniques such as the anonymisation or pseudonymisation of data. However, respondents from research backgrounds suggested that although in many cases they do not need to know who an individual is - and as a rule are not at all interested in this - in many cases it may be necessary to trace or contact the individual. For that reason, full anonymisation was often undesirable. There was strong agreement that more use should be made of encryption, as this can go a long way towards safeguarding patient confidentiality and the scientific integrity of the data, whilst ensuring that data could still be de-anonymised where necessary. Pseudonymisation was felt to be particularly useful because it removes explicit identifiers from a dataset yet allows information about the same person to be linked, by allocating a unique identifier to him or her. A trusted third party could hold the 'key' that links real identity to pseudonym.

75. In the medical arena, there was widespread agreement that it would be harmful to research and to public health more widely to insist on full anonymisation as there were many instances in which it might be necessary to track or identify patients or research volunteers. In its submission, the PHG Foundation suggested that those charged with research governance, such as research ethics committees, have traditionally judged anonymisation by the simple test of whether those involved in research were reasonably likely to identify the data subject or not. For the most part, it was suggested, this pragmatic approach seemed to respect individual privacy. However the threshold for advice from the Information Commissioner's Office was said to be much higher, requiring that the data processor considers the means reasonably likely to be used by a person who is determined to identify the data subject, such as a hacker or investigative journalist. PHG said that whilst data processors clearly have an obligation to assess the effectiveness of their data security systems and processes in the context of rapid technical change, its view is that increased sanctions should be placed upon those who deliberately seek to de-identify personal data without legitimate cause, rather than seeking to over regulate at the other end.

Section 6: International comparisons

76. In the final section of our consultation document we solicited examples of other jurisdictions where the law or best practice had developed in particularly useful ways. Although we received some interesting submissions, we received less evidence in response to this section than we did in response to the others.

77. In general, it was thought that the UK had adopted the European Data Protection Directive in a pragmatic and balanced way, making the country attractive to business.

> "Despite any criticisms we may have, in comparison to many other countries, the UK is in many respects an international leader in the regulation of personal data and engagement with business issues pertaining to data sharing in the public and private sectors."
>
> **Confederation of British Industry**

78. Several respondents did point to examples of foreign jurisdictions that had adopted particularly useful laws and practices. Most comments were addressed either at the overarching frameworks (or even guiding philosophies) present in different countries, or at specific laws, rules or devices said to be in common use overseas. Many respondents commented on the differing approaches adopted by the United States of America and the European Union. There was said to be a difference in fundamental attitudes towards the management of personal information and privacy matters here, with the European Union, and some other jurisdictions, following a legislative path underpinned by the view that privacy is a human right; but with the US still typically regarding personal information as belonging to the organisation, with special obligations of stewardship in terms of its handling and management. The end result (i.e. that personal information has to be dealt with securely) might often be the same, but the route to get there was seen as being very different.

79. When looking at data sharing frameworks, some respondents pointed towards other Commonwealth jurisdictions as having sensible and practicable measures in place. Canada was cited by some as being a bridge between the approaches adopted by the EU and US, and Australia was used as an example by others, particularly in terms of its attitudes to health and other administrative data. Some respondents also cited the broad framework in New Zealand, pointing to the way in which information management law is brought together in a simple but very effective way.

> "The New Zealand Information Privacy Act 1993 is seen as a successful legal framework for sharing and protecting personal information, and could be useful in a UK context."
>
> **British Computer Society**

80. Respondents made a number of observations about data protection in other countries from which they thought the UK could learn. Respondents pointed to:

- the German experience of laying down a specific requirement for informed consent for cancer registration, which led to the effective collapse of the system. Similar problems also occurred in Canada and in Hungary - where patients either withheld their consent or doctors did not ask for consent in the first place;

- the advantages and disadvantages of the breach notification provisions in force in the United States of America and Canada. In particular, respondents focused on the trigger points for the notification of a breach, and the issue of who the notification should be made to - for example, the regulator or the individual or both. There were also wider issues about whether people would become immune to breach notifications, meaning that they may not take notice when there is a genuinely significant breach. Some respondents also expressed concern about the burden on business;

- the presumption in many European countries that population and business registers should be available to the central statistics office for national statistics purposes. It was suggested that the use of administrative data for statistics is, in many countries, assumed, and that other jurisdictions in the EU have implemented the provisions in the EU data protection directive more positively from a statistics and research perspective than is the case in the UK;

.

- the powers of regulators in other jurisdictions. The common theme was that the UK's Information Commissioner has substantially weaker powers than some of his international equivalents. For example, the Canadian Federal Privacy Commissioner was said to have the power to audit organisations, and the Ontario Privacy Commissioner the power under the Personal Health Information Protection Act to fine institutions up to $1 million (Canadian dollars);

- the Dutch *e-Citizen Charter*, which sets out ten rights for citizens and ten corresponding duties for government in connection with the use and sharing of personal information, and the subsequent *Citizenlink* programme that seeks to implement it; and

- the wider use of Privacy Impact Assessments in countries like Canada, particularly the model adopted by Ontario's Privacy Commission, which involves the use of federated PIAs.

Annex D - Workshop notes

To help inform the review we conducted a number of workshops to bring together people from a range of disciplines and sectors - including government, the financial industry, the retail sector, academia and voluntary organisations - who had a particular interest in the sharing of personal information and the problems and opportunities that such sharing can entail. Delegates were encouraged to exchange views and debate with each other, focusing in particular on any *problems* that they perceived as existing in the current legal and cultural climate; and potential *solutions* to those problems. Below is a note summarising the major issues coming out of the series of workshops, which was prepared by the independent facilitator (Ian Gambles) who chaired each of the sessions, together with minutes compiled by the review's secretariat of each of the individual workshops. There is also a minute provided by Intellect, who facilitated an additional workshop for their members. We are very grateful to Ian and to Intellect for the work they have done for us, and for allowing us to publish their thoughts here.

Summary note - Ian Gambles, 21 April 2008

This short paper is a personal view of the key themes to emerge from the seven workshops which I facilitated for the Review, and the more promising solutions advocated in them. It starts with a look at the philosophical background, then turns to the specific practical issues identified, and concludes with solutions.

Philosophical background

Data sharing generates emotional heat because it is so bound up with fundamental tensions in British political culture. The debate is indeed part of a struggle over the history and direction of politics. To a unique extent, there is in this country a permanent tension between a powerful libertarian instinct and a commitment to social cohesion and democracy. Not only is it not the place of a review of data sharing to try to resolve this tension, it would also be the wrong thing to do. However much the argument might make us squirm sometimes, it is a healthy state of affairs, and the tension must be allowed to continue indefinitely and form the background to political decision making.

Loud voices in the workshops defended individuals' rights against the state, and vigorously expressed a commonly held, and perhaps increasing, citizens' distrust of government. Is my DNA not mine? Who is the state to take it and keep it without my consent merely because I was once at a police station? Most of us do have something to hide - not a crime, but nobody else's business - so why should my every bus journey be tracked on a card, my data trawled through in the search for wrongdoers, my personal information passed from one agency of the state to another without my agreement? Is it any wonder people are distrustful of the data-rich state when they can turn on their TV and hear DVLA or TV Licensing telling them menacingly that "our computer knows where you live"?

Equally loud voices in the workshops asserted the legitimate claims of society, the view that public servants trying their best to protect the public against crime, to provide better public services, to improve public health and develop new cures for disease, and to get better value for taxpayers' money, are being hampered in all these endeavours by an

ambiguous legal framework and a zealous privacy lobby. Why should an individual be allowed to render aggregate medical data invalid for research purposes by withholding consent for use of "their" pseudonymised records? Why should a local authority not use its accurate data records from the electoral register to improve its management of access to social housing? Why should HMRC inspectors not report health and safety violations?

I am convinced this is the dialectic in which the way forward must be situated. This is not about data as property - that is the wrong approach. It is about individual rights, and the limitations on them which can properly be set in the interests of society.

Practical issues

Many at the workshops on both sides of the argument stressed that, while the principles were important, the issues were not abstract but practical, and the review should set a practical direction. I was particularly struck by the repeated observation that many data controllers at a working level - in agencies, local authorities, health trusts - were "all at sea", and were making decisions on the back of a limited understanding of a complicated law interpreted by a plethora of ambiguous guidance. No surprise then if social benefits and individual rights both suffer from erroneous judgements depending on whether the decision maker feels more anxious about pressure from other agencies for access to data or about the fiery breath of the Information Commissioner on their neck, or on whether Soham murders or HMRC disks are more prominent in the news.

These are some of the most significant practical issues which were identified:

- *Lack of transparency*. Individuals' personal data is being used for purposes they have no idea about, "popping up in unexpected places". While some linked this to the issue of trust, in my opinion that is a mistake. Transparency may or may not create trust; but it is surely a right.
- *Poverty of guidance.* Much of the available guidance was said to be "useless", evasive and risk-averse. Officials will always have to use their judgement in many cases, yet there is no generally accepted statement of the principles on which these judgements should be based, or any clear articulation of either the benefits or the harms from data sharing.
- *Legal ambiguity.* While the DPA was generally felt to be fit for purpose, there were some areas where more clarity would help, notably the force of the second principle and the legal status of pseudonymised and anonymised data, particularly for medical practitioners.
- *Subject access.* It is not easy enough for those who want to exercise their subject access rights to do so. The process is cumbersome and costly, there are better options available in the internet era, and organisations are not attaching sufficient priority, e.g. in systems design, to giving people access to their own data.
- *Inadequate sanctions.* Penalties for breaking the law are too light, redress too difficult to obtain, the regulator's powers too weak. On the other hand, others felt that sharing too much was sanctioned less severely than sharing too little, and there was little reward for getting it right.
- *New technological possibilities.* Some pointed to new and emerging technologies, such as user-centric identity management, as offering tools to enhance individual control over personal data. There is a risk, however, that over-reliance on technology-based self-protection could disadvantage the less technically sophisticated, including of course vulnerable people.

- *Spurious consent.* There was no agreement and little helpful thinking on the practical scope for extending the criterion of consent. All agreed, however, that it was wrong for the individual to be taken to have given their consent when faced with a barrage of small print to which s/he had to agree in order to access everyday services.
- *Data accuracy.* It is too hard both for individuals and for public authorities to correct inaccurate data (or delete expired or redundant data). Data sharing restrictions prevent authorities using their better data sources to correct others, while unco-operative authorities offer scant provision for individuals to do it.
- *Data export.* Export of personal data to countries with less adequate data protection regimes needs to be more tightly controlled in the era of overseas data centres and the World Wide Web.
- *Data security.* Government's recent record on data security, and its work on information assurance, is not delivering public confidence in safe data sharing.

Possible solutions

The range of solutions offered by participants at the workshops did not exactly dovetail with the problems they identified, and the report will need to be more thorough and precise. The necessary corrective action for some of the above issues is fairly obvious and is not spelled out here. Many of the suggestions which were made seemed sensible and proportionate and may offer the basis for a reasonable package of improvements. These struck me as the more important elements to consider:

- *Statements of justification.* Organisations should be obliged to state publicly in a Code of Practice the uses to which data they collected was put, including any data sharing, to justify that use in terms of the public interest, and to be able to demonstrate that they actually did use/share data in that way.
- *Highway Code for data protection.* The regulator should publish a plain English guide to the principles and practice of data protection and data sharing, with a view to it becoming authoritative and widely used by data controllers to inform their decisions.
- *Privacy Impact Assessments.* PIAs should be required in government at policy stage, and perhaps carried out by independent practitioners. (My experience of Diversity Impact Assessments suggests this would certainly raise the profile of the issue, at the cost of much added bureaucracy and tick-box compliance, and to the profit of niche contractors).
- *Parliamentary oversight.* Parliament should take a stronger hand, perhaps by legislating a statutory framework, based on a typology of sensitivity, for permitting or forbidding data sharing in defined situations (and perhaps in defined functional zones), or perhaps by approving Codes of Practice.
- *Regulatory powers.* The sanctions, investigative powers and resources of the Information Commissioner should be increased. (Analogies were often drawn with the Health and Safety Commission, although personally I do not think much of the comparison. In my view the ICO needs more resources to do more audit, enabling and advice, not more enforcement).
- *More training.* The above measures could all be made much more effective by enhancing the provision of data protection training, and awareness raising, provided to public sector staff and available in the private sector.
- *Encourage online access.* Organisations should be encouraged, and good practice guidelines developed, to offer opportunities where appropriate for individuals to exercise their subject access rights online and without charge, and to correct their own personal data

- *More proportionate intrusion.* Government should recognise people's legitimate discomfort with public authorities' intrusive use of personal data, start making sensible compromise decisions and drop the evangelical tone in selling the benefits of data sharing.
- *Greater range of civil penalties.* US-style provisions for mandatory notification and rectification of data protection breaches could be introduced, along with provision for a small statutory compensation payment to all individuals affected.

Workshop 1 - 29 February 2008

Attendees

Belinda Crowe, Head of Information Rights Division, Ministry of Justice
Caspar Bowden, Chief Privacy Officer, Microsoft
Graham Sutton, Constitution Unit, University College London
Jane O'Brien, Head of Standards and Ethics, General Medical Council
Lynn Evans, Information Compliance Officer, Manchester City Council
Professor Charles Oppenheim, Department of Information Science, Loughborough University
Stewart Dresner, Chief Executive, Privacy Laws and Business
Stuart Lynch, Consultant, Privacy Laws and Business
Superintendent Patricia Ogden, IMPACT Programme Manager, Hampshire Police
Trevor Bedeman, Managing Consultant, Financial Information Markets

Introductions

1. It was explained at the outset of the meeting that the discussion would form part of a series of workshop sessions designed to feed into the evidence being gathered by the Data Sharing Review. The objective of the workshop was said to be to give those present an opportunity to set out and discuss views and ideas on the use and sharing of personal information, including the context and method; the benefits and risks for society and the individual; and possible changes to current law and policy. In terms of structure, it was proposed that the first hour of discussion should focus on 'the problem' (i.e. is there anything within the current framework of law/policy/practice that causes concern, and if so, what is it?); while the second hour of discussion should focus on 'the solutions' (i.e. how can we remedy anything that is thought to be a problem?).

'The Problem'

2. Discussion moved to identifying issues thought to require attention:

    - it is often said that society needs to 'balance' (a) the benefits that can accrue by sharing personal information against (b) the need to protect individuals' rights to privacy - in the context of the legal framework to some extent imposed upon us (with reference in particular to the Human Rights jurisprudence from Strasbourg and to Community law from Brussels), how much licence do we in the United Kingdom have to make that balance and (assuming there is some licence) where should that balance lie?;

- assuming that data sharing is a positive thing, how can we help to increase public confidence (and therefore trust) in order to allow the anticipated benefits to accrue - particularly in a context where Government seems continually to be pushing the boundaries of the types/quantities of data it wants/needs to control, without necessarily establishing a solid competence track record with the data it already controls?;

- to what extent are 'transparency', 'control' and/or 'consent' important, and in particular are they of themselves (individually or collectively) any or any sufficient safeguard/public protection, or do we need other regulatory devices, for example like those currently found in the 'Health and Safety' field?;

- the "philosophical" debate about the perceived increase in what can generically/colloquially be described as a 'surveillance culture', including the issues at the heart of the topical European Court of Human Rights case on DNA record retention by the police (*Marper* -v- *United Kingdom*[1]);

- what are the benefits/otherwise of anonymous or pseudonymous data sharing, and if there are benefits, how can we make sure they are achieved?; and

- are the issues different when the sharing of personal data is designed to achieve public protection, as opposed to being designed to help facilitate improvements to services received by individuals or groups of individuals - or, framed a different way, is there an important distinction to be drawn between situations where data is shared for the benefit of specific/defined individuals (e.g. to improve a service provided to the data subject) and situations where data is shared with a result that is contrary to the interests of the particular individual (e.g. when data sharing during a criminal investigation leads to the arrest and conviction of the data subject)?

3. Having briefly discussed that broad range of issues, discussion then focused on the issues felt to be most important.

Pseudonymised Data

4. Attention was drawn to Recital 26 of the European Directive on the protection of individuals with regard to the processing of personal data (Directive 95/46/EC), which provides that whereas any personal data that is *anonymised* shall not fall within the scope of protections afforded by the Directive, any other personal data shall do. So, under the Directive, if there is any information concerning an identified or identifiable individual (that is to say identified or identifiable by the data controller "or by any other person"), then that information will be covered by the principles of protection therein set out. It was suggested that the status of 'pseudonymised' data was

[1] S. and Michael Marper -v- United Kingdom, European Court of Human Rights, Application Numbers 30562/04 and 30566/04

relevant, particularly in the context of dynamic IP addresses - codes that identify accounts accessing the internet (so normally either individuals or small groups of individuals, like families) and which e.g. enable records to be kept about which e-accounts have logged on to what internet sites and/or purchased services/products. The suggestion was that although under the European Directive, the link between personal identities and dynamic IP address identifiers (known only by the relevant Internet Service Provider and not known e.g. to individual website/service providers) was sufficient to establish information as personal data, under the UK's Data Protection Act regime things were less clear. The retention of dynamic IP addresses had significant privacy implications. This seemingly less stringent approach under UK legislation could spell trouble at some future point. However, it was also suggested that, at least insofar as the genetic/medical research community was concerned, the UK did in practice adopt the more stringent approach of the EC Directive when determining what constituted anonymised data and what did not.

5. In terms of 'problems' caused in this area, it was suggested that e-profiling by e.g. marketing companies could lead to situations where (based on particular individuals' web browsing habits or otherwise) adverts offering services/products could be sent direct to individuals with different terms and conditions deemed to apply. So some people could be offered a service at a higher price because they were perceived as easy targets. This process, which would necessarily have to be secretive and kept from the individuals concerned, would very much go against the spirit of transparency, where all individuals are supposed to be able to access any information held on them and see in what way(s) it is being used.

6. There followed a brief discussion on the extent to which e-profiling in this vein could be used, although there was no clear consensus of opinion. Discussion touched on whether e.g. law enforcement agencies should be able to use intelligence from dynamic IP addresses to investigate people accessing illegal material on the internet (the example used in discussion was child pornography). It was said that if an individual uses a credit card to purchase access to illegal material over the internet, the credit card company would have a legal obligation to disclose that information to the relevant authorities. But should data be made available to the authorities even where there is no monetary transaction and so no credit card records exist? There was no substantive answer provided by those present to the hypothetical questions posed.

Public Protection

7. There seemed to be a clear consensus around the proposition that sharing data with the objective of protecting the public was distinct from sharing data in order to target improvements to an individual's service. The following points were made during discussion:

- several attendees suggested that CCTV gave rise to valuable opportunities to help detect/prevent crime, particularly terror-related and child protection activities, although some suggested that the public would be likely to agree with police access to CCTV

information to e.g. check whether someone is evading car/road tax and/or driving without insurance;

- there was thought to be an important distinction between, on the one hand, affording the police access to data captured by CCTV networks in case-by-case situations and, on the other hand, allowing the police open access to trawl the information, 'fishing' for potential criminal activity of whatever scale/severity - with the former generally accepted as 'right' and the latter generally thought to be 'wrong' (in the main because of the principle of presumed innocence);

- the police were said to be developing transparent guidance and codes of practice so that people could see the limits imposed on individual officers/employees but there was no agreement amongst all attendees that this afforded any or any sufficient protection for the public against potential abuses;

- concern was expressed about "function creep" whereby new technologies are developed on the explicit basis that privacy will be respected but subsequently, once authorities realise the full potential of these technologies, privacy safeguards seem gradually to be eroded - the examples of London's Congestion Charge cameras and the NHS' Summary Care Records initiative were cited in support, where in each case clear undertakings seemed to have been provided at the outset on e.g. the limits on data retention but where subsequently developed practice appeared to be in breach of those undertakings (or at least the spirit of those undertakings). In the case of the Summary Care Records, clear opt-outs are available. However, this is not the case in relation to secondary usage of health data - to which it was suggested the Police could gain access; and

- the importance of non-electronic records/data was highlighted, particularly as in public sector organisations there is often a lot of personal information stored in hard copy filing systems - and in this context the danger of making the debate too technical was also outlined, with the suggestion that if e-specialists hijack the debate, the basic principles that ordinary people can understand about the rights and wrongs of processing personal information could get lost, to the great disbenefit of society more generally.

Consent

8. In a world of fast-paced technological change, where the so-called 'Moore's Law' (roughly to be translated as meaning that every two-year period will see a doubling of the number of transistors on computer chips, thereby increasing the power of computers to process information by that same factor of two) is continuing as predicted, and where the universal currency of the credit card facilitates global on-line transaction completion seemingly with ease, the issue of individual data subjects giving consent ahead of their data being processed was agreed as being ripe for review.

9. It was suggested by a number of those present that what used to be understood as ‘consent’ might better be styled in the modern world as ‘notification’: individual data subjects should be told exactly which data of theirs are held and there should be transparency around why those data are held, and for how long they are expected to be retained. There could (and should) then be appropriate mechanisms for data correction or challenge by the data subject, if/as necessary. But most present agreed that it would be impractical to insist upon true ‘consent’ before data collection and retention begins, particularly in the context of some of the larger data handling operations under way in the modern world.

10. One specific example discussed was that of financial transaction data in the European Union. A hypothetic scenario was suggested in which *A* (located in England) transacts with *B* (in Germany) under a standard consumer contract. *A* pays *B* with a credit card via *B's* website. So far, so good in terms of an intra-EU transaction that will be governed by the protections set out in the Directive. But assume that the credit card is provided by a company (*C*) based in the United States of America. The transaction between *A* and *B* would be processed via *C's* electronic payment hub in the States. As the details of the transaction pass through the territory of the States, the US Government could access the records freely under powers vested in it by e.g. the USA PATRIOT Act 2001. Data processing beyond that point in the USA would then not be protected under the terms of the Directive and/or English/German national law. Because the very essence of what the US Government and/or its agencies would be doing would likely be covert, there was likely to be very little if any accountability in the system - and that was felt by at least some of those present to be dangerous.

11. Several of those present agreed that ‘trust’ was an essential element here: many citizens might feel cynical about ticking a box to ‘opt-out’ of a data sharing scheme because of past experience where they have asked to opt-out but then still received unwanted mail from related marketing companies. So many present said that effectively policing whatever regime is in place is imperative.

12. In the context of e-data processing, there was a suggestion that the data protection/management’s regime could more usefully focus on the user as a way of engaging that user and gaining their trust. For example, if data subjects are continually completing transactions on-line and conducting all sorts of other business electronically, why does the data protection regime prevent them from seeking to make their Subject Access Request (SAR) on-line? It was noted that, in the UK at present, a SAR tends to take around a month to be answered, it costs the applicant £10 for the privilege and the process can be very labour intensive for the data controller. But technology exists (or if it doesn’t, it soon could) to search for relevant information almost at the drop of a hat. So the question was posed: why cannot automated systems be tasked with trawling for and providing the information requested via a SAR?

‘The Solution’

13. There was a suggestion (although not one that was universally accepted) that transparency was the critical issue, particularly in terms of data sharing where the object is public protection. As an example, those present discussed a police initiative concerning data sharing between local forces, which is organised under the auspices of the IMPACT programme. IMPACT is designed to improve the ability of the police service to manage and share information to prevent and detect crime and provide safer communities. It was explained that, currently, information held in one force's local system is not available to officers in other areas. By giving forces the ability to find and access operational information across England and Wales, the IMPACT Programme is attempting to transform policing in the UK. The key elements of the IMPACT programme are: Management of Police Information (MoPI), aimed at helping forces to meet common standards for police information management through a statutory code of practice and associated guidance; IMPACT Nominal Index (INI), enabling forces to establish whether any other force holds information on a person of interest; and the Police National Database (PND), which is being designed to provide a single access point for searching across all of the forces' main operational information systems. The potentially massive databases, accessible in theory by many thousands of police force employees up and down the country, will clearly be a major step beyond what the status quo allows and, as such, it was explained that issues on the implementation of the programme were out to consultation. It was explained that the police hope that transparency will be key to ensuring public trust although it was commented on that the consultation did not seem to have developed any significant public profile and so it amounted in effect to an internal police discussion which was perhaps unlikely to engender great transparency or trust.

14. Discussion also covered the applicability of the second Data Protection Principle (see Data Protection Act 1998, Schedule 1, Part I, paragraph 2) and whether it was understood sufficiently well what the term ‘compatible’ meant in that statutory context (in particular because there had been little if any authoritative jurisprudence on the subject since the ’98 Act become law); and about the proposal for ‘positive justification’ (i.e. an obligation, in addition to the protections currently afforded by the data protection regime, on data controllers to support any proposal to share data with a third party on some positive basis, whether by reference to the public interest or otherwise).

15. All present seemed to agree that the statutory regime had to remain technologically neutral, insofar as the law could not be used to mandate specific technological solutions when technology could change so much faster than the law. Some of those present reiterated the call not to focus exclusively on e-solutions, arguing that to do so may be to disenfranchise a significant section of the population from the protections and rights afforded by the law. And where it was necessary to focus on e-systems, it was suggested that it had to be remembered that a large number of legacy systems currently existed, for example, throughout the public sector. If

technological change were required, it would take some time to come about, as reform like that costs time and money.

16. The discussion session closed when each participant was given the opportunity to mention one specific change that they would like the Review to consider as a recommendation when it (the Review) comes to report. The following suggestions were made:

- two of those present called for the 'positive justification' model to be introduced to the statutory framework, obliging those intending to share personal information to put forward a case as to why that sharing would be beneficial;

- one attendee urged the Review to recommend giving clarity to the 'second principle' and in particular to the doctrine of 'compatibility';

- one attendee urged for more public debates prior to new data sharing schemes being set up;

- one attendee urged the Review to recommend that there be more clarity and guidance specifically on data sharing, including when sharing would (as opposed to would not) be allowed and simplifying the legal authorisation for sharing information;

- one attendee said that the idea that transparency in and of itself would be sufficient to engender trust was a nonsense and that what was required was real empowerment for individuals so that they could protect themselves under the law;

- one attendee said that there should certainly not be any restriction of the types of information that can currently be shared and that published protocols and codes of practice would help to increase transparency and therefore public trust;

- one attendee suggested that the powers of the Information Commissioner's Office and of the courts should be increased and that there should be a new Central Register of all data controllers showing each of their data sharing partners; and

- one attendee suggested that the statutory powers to force compliance with the data management regime should be increased in line e.g. with the Health and Safety Executive ("it's only when threatened with prison that people start to take notice"), and suggested that cross-Government IT policy should be sorted out so as to avoid fragmented contract providers all servicing widely divergent systems that will never properly integrate with partner agencies should they want to share data efficiently in the future.

Workshop 2 - 6 March 2008

Attendees

Dr Adam Warren, Loughborough University
Dr John Parkinson, Medicines and Healthcare Regulatory Agency
Gareth Crossman, Liberty
John Turner, Association of Electoral Administration
Malkiat Thiarai, Birmingham City Council
Phil Walker, Department of Health
Professor Charles Raab (ret'd), University of Edinburgh
Richard Jeavons, Department of Health

Introductions

1. It was explained at the outset of the meeting that the discussion would form part of a series of workshop sessions designed to feed into the evidence being gathered by the Data Sharing Review. The objective of the workshop was said to be to give those present an opportunity to set out and discuss views and ideas on the use and sharing of personal information, including the context and method; the benefits and risks for society and the individual; and possible changes to current law and policy.

2. In terms of structure, it was proposed that the first hour of discussion should focus on diagnosis of 'the problem' (i.e. is there anything within the current framework of law/policy/practice that causes concern, and if so, what is it?); while the second hour of discussion should focus on 'the solutions' (i.e. how can we remedy anything that is thought to be a problem?).

'The Problem'

3. There were obviously a number of benefits, opportunities and risks associated with data sharing, but what were the current problems or issues that needed to be addressed? Did the current regime need to change, and were there currently any areas of imbalance between realising the benefits achievable through data sharing and the need to sufficiently safeguard against any associated risks? To inform the group's discussion of these issues, concerns raised at the previous meeting were shared with the group.

The legislative framework

4. It was argued that, ten years on from its introduction, the Data Protection Act (DPA) may no longer be fit for purpose. The capacity for storing and sharing data had dramatically increased due to technological developments, an increase matched only by the Government's desire for greater data sharing to fight crime, prevent terrorism and deliver services, and as such the DPA would need to be reviewed in this modern context.

5. Judging whether to share or not to share personal data was highlighted as a difficult decision to make, something not helped by the ambiguity of the DPA. This caused great anxiety within organisations that shared data. This ambiguity was further compounded by the complex framework of data sharing legislation such as statutory gateways and restrictions, and the laws of confidentiality.

6. The idea was raised of having a 'free for all' approach to data sharing, where everyone had the power to share data with anyone they chose too, with clear accountability, transparency and recourse. However most thought there was little appetite for this and that there was a tension between regulation and getting the job done.

Guidance

7. Part of the problem lay in the concept of 'balance' - this could only be determined by looking at the nature of the data and the context of the data sharing. As such, in the public sector, guidance produced from the centre had been less helpful than guidance which focused on the point at which the subject met the data controller (front line services) and cross-service sharing. Guidance tended to be risk-averse, covering when not to share data rather when to do so.

8. Front-line staff would rather be blamed for sharing too much data and receive a minimal penalty from the ICO ('a slap on the wrist') than risk serious consequences resulting from not enough data being shared.

Powers of the regulator

9. There was general recognition that the ICO required greater powers and more funding, akin to other regulators. In particular, the ICO's seeming inability to influence major public sector data sharing initiatives, such as the eBorders Act, was highlighted as a problem. Government could create powers that allowed it to share any data with anyone for any purpose, which then made any sense of proportionality difficult to enforce. Creating these types of powers risked a loss in trust in the Government to use people's personal information fairly and proportionally, and the ICO's ability to regulate data sharing in the UK.

Public perceptions

10. Generally, less guidance from the centre may be a good thing as 'Government' was less trusted by people than locally-provided services. In healthcare, there had tended to be efforts made to avoid the appearance of a direct link with central Government. The health sector already had an ethos in place built around confidentiality that didn't require legislation, and was not affected by changes in technology.

11. Trust, or an individual's willingness for their information to be used or shared, was also inherently linked to the benefits received from sharing personal details. For example, people would be happy to fill in a form when buying a mobile phone and contract. The use of the electoral register for purposes other than voting was a case in point. People associated registering on the Electoral Roll with receiving the 'benefit' of being able to vote, and felt uneasy when their information was used for purposes that did not lead to any clear benefits for them or that were completely unconnected to the primary need for collection. Unless the benefits are clearly tied to the use of data a crossroad is reached that may be difficult to overcome.

12. Local authorities had problems balancing the need for transformational/joined-up government with data protection, as often data may be shared simply to ensure records are accurate, rather than for a clear, direct benefit for individuals. In this respect, access to the electoral register and council tax data is important to ensure data quality. However, consensus was not reached on this issue with some attendees expressing the view that information collected under a statutory power should not be used for any unconnected purpose.

13. The terminology used in data sharing, such as anonymisation and pseudonymisation, could also be problematic as people did not know what they meant, and so explaining what the risks or benefits of any sharing of data was difficult.

14. Advancements in technology had also raised anxieties amongst the public. People were more aware of the public and private sectors increased capabilities to use, share and manipulate data. However, policy makers had not kept up to speed with this growing awareness and so did not properly think about how to address peoples concerns and make new uses of data more transparent and linked to clear benefits.

Privacy Enhancing Techniques

15. Patients were often surprised that data isn't being shared and used more already in the health sector. Again, context was important, particularly as there was a greater capacity for linking and anonymising/pseudonmising data. For example, sharing data was generally approved when it was on medical safety grounds, but less favoured when used for pharmaceutical pricing, whether anonymised or not.

16. Privacy enhancing techniques may not always be the answer. The reality is that if some temporal data were known, even if anonymised, this could be matched with other data to identify people, without even having to link very complex datasets together. It may therefore be incorrect to tell people they cannot be identified when they actually could be. The DPA would not stop this and data handlers had to adopt the highest levels of probity and standards, with severe sanctions if any rules were broken.

Data Profiling

17. Sharing data for profiling purposes had become more of an issue. Profiling could mean simply data matching, but could also mean much more than that and proportionality was often viewed as an afterthought. As data sets grew larger, more of this profiling would have to move to automated processes and it was questionable whether the current ideas of proportionality and the 2nd Data Protection Principle would be suitable to be able to manage this?

18. Profiling of some description occurred now, for example in local authorities who want to establish who uses services. However, the connotations associated with profiling that had come about through concerns over the development of a surveillance society had made this type of work difficult. This was an example of where national data sharing initiatives such as ID cards or data sharing to tackle crime and terrorism had a detrimental impact at the local level and could stop real benefits being realised.

Consent

19. There was a discussion on the importance of 'consent', with some attendees agreeing with the view that consent was "important, but not *all* important". One attendee suggested that the concept of consent was "cheapened" in situations where it was sought from the data subject but, irrespective of the data subject's response, the data could and in all likelihood would, be shared on other grounds in any event. Some attendees agreed that the giving of consent was now in many ways seen as being "part of the deal": individuals receive the benefit of certain public (and other) services and, in return, they are required to give permission for their personal data to be shared.

20. The issue of consent was often put in the 'too hard' category. This may have been due to misunderstandings of terminology ('informed', 'explicit' etc), the need to make a decision in a high pressure environment (such as dealing with a seriously ill child), and that consent may not go far enough to meet requirements. Consent could be problematic, and people were generally only concerned about having their consent sought in certain circumstances and only cared about what happens to their data when they needed to. Pushing consent onto people who have no real interest may therefore be difficult.

21. Society increasingly appeared to be moving towards using more opt outs. This would make the delivery of efficient public services difficult to achieve, and determining the context of when to use consent and when it would not be appropriate was important. Part of the problem was that people were not sure what opting in or out of something really meant, as seen with the electoral register which can be unclear about what the edited register is and who it was used by. Opt outs of the electoral register had increased slightly over the years, but this lack of awareness of the implications of being on the edited register remained. There was marked increase in opt outs when

Watchdog ran a story on the edited register and what it was used for, highlighting the issue that opt in and opt outs weren't properly understood, or properly explained, but when they were the results might be very different. Organisations should never take peoples trust or understanding of consent for granted. Instead there should be better and clearer duties of responsibility placed on data controllers.

22. Among the group there seemed a broad consensus that there was little appetite for "radical reform" of the consent rules, e.g. either abandoning the concept of sharing by consent in its entirety (and so sharing on other grounds instead) or moving the opposite end of the spectrum and mandating 'informed consent' in all but exceptional instances of personal data sharing.

Cultural and institutional

23. In the public sector, there appeared to be tension between different departments mindsets on data sharing, for example, the Department for Health and Home Office effectively sit at different ends of the spectrum (Health being overly restrictive, while the Home Office and law enforcement agencies were too eager to use and share data). As such there appeared to be no common Government approach to data sharing and a lack of a cross-departmental perspective, something that could be rectified through the creation of a Parliamentary select committee overseeing government data sharing activities to ensure a joined-up governmental approach.

24. Many of the problems within Government in this area had been around for years, which suggested there may not be a simple, one-size-fits-all, solution, but there did need to be real drive in this area from the Permanent Secretary level that dealt with on the ground situations and problems.

25. The Bichard Enquiry highlighted the tendency of public sector bodies to lack an institutional memory when it came to procedures, guidance and rules, which could in part be explained by high staff turnover. The basic principles of data protection and data sharing need to be instilled into the culture of an organisation to prevent this. The private sector seemed better at achieving this as there would be risk to a company's reputation if they got data protection wrong - something which may be lacking in the public sector.

26. There was a tendency in many sectors, private and public, to see data sharing as being a contest between privacy and benefits. This was a cultural problem and there needed to be a shift in values that saw the protection of privacy as also being beneficial, not just to the individual but also to society in preventing discrimination and retaining or gaining trust.

27. One difference between the public and private sectors that impacted on culture was responsibility and reputation. BUPA, for the example, would not want to become the 'next HMRC' as this would cause significant damage to their reputation, and undoubtedly heads would roll. This created a culture where properly protecting data

was a major priority, and one that the Government could learn from. Possibly Permanent Secretaries should be responsible for data protection, and face the sack if major breaches occurred. Government should be more concerned about damaging their public reputation as competent keepers of data to ensure the willing co-operation of people to provide personal information.

'The Solution'

28. Much could be achieved via pseudonymised data sharing to help protect privacy. Many objectives of an organisation could be achieved using this type of data, with individuals only being identified where absolutely necessary. However, pseudonymisation required accurate, high-quality data, which could not always be guaranteed. Best practice and guidance was required for these types of techniques.

29. Guidance was helpful, but was often ignored. Most present felt that a move towards a risk management approach was required, where guidance was given on how decisions should be reached, backed up with incentives for getting data protection and data sharing right, perhaps by relating it to career progression, or by having some kind of recognition or bonus scheme in place.

30. To ingrain the principles of appropriate data into organisational culture (particularly in the public sector), regular training could be introduced, perhaps via yearly seminars or training courses, or on-line self assessment programmes. Many of the attendees highlighted the Health and Safety environment and culture as a model to try and emulate in data protection.

31. There should be greater direction in the Government's overall data sharing strategy that moved away from sector specific mindsets. A data sharing select committee might be one way of achieving this, as would the establishment of a data controller/ Caldicott Guardian role in Central Government.

32. The discussion session closed when each participant was given the opportunity to mention one specific change that they would like the review to consider as a recommendation when it (the review) comes to report. The following suggestions were made:

    - Data sharing should be reigned in. Tightly arranged data sharing arrangements for the key partners involved in delivering a particular service should be created, and activities should not go beyond those arrangements.

    - Legislative changes for access to the electoral register and council tax data need to be completed to allow local government to have clear basis for accessing and sharing data to assure data quality.

    - Professional skills in making risk-based decisions about data sharing need to be cultivated. Privacy Impact Assessments could be part of that process, as

long as they did not become a box ticking exercise. The culture needs to change from blame to responsibility.

- Clear, authoritative guidance, that does not institutionalise ambiguity, coupled with transparency and good practice.

- Government and policy makers need to get the message across that the DPA and data sharing are not in themselves bad things.

- Better data protection legislation is required that is suitable for the modern data sharing and technological context, backed up by a strengthened and properly resourced ICO.

- There needs to be greater transparency and accountability. Statutory gateways need to be made tighter, where the scope of purpose is limited and where data sharing does not go beyond that agreed with Parliament.

Workshop 3 - 13 March 2008

Attendees

Esther George, Crown Prosecution Service
Jane O'Brien, General Medical Council
Marc Taylor, Department of Health
Peter Norris, Local Government Association

Introduction

1. The context of the review and the purpose of the workshops were explained to those attending. The workshop would focus on two areas; the problems, or rubbing points in the current data sharing regime, and the possible solutions to any problems identified.

'The Problem'

The Data Protection Act and confidentiality

2. As a problem, one attendee said there was a lack of understanding of the Data Protection Act in the health sector which led to data being incorrectly shared or appropriate data sharing not taking place. This was compounded by the lack of clarity between the interaction common law and DPA - the DPA was seen as being more permissive about the secondary use of data than the common law which called for justification of use rather than a proportionality test. This confusion and lack of clarity made decision making difficult for doctors.

3. Medical research was considered as a medical purpose under the DPA, but when people interact with the health sector they generally believe that their data will remain in confidence with the care team and will not necessarily be used for research purposes.

4. Another attendee agreed, stating that the duty of confidence applied universally, but doctors felt there was a specific duty of confidentiality that applies to them and which took precedent over the DPA. As such they can feel that data cannot be used when it actually could be. The problem was a lack of understanding about specific legislation that deals with context specific issues, and doctors thinking that the duty of confidentiality trumps all other law. This could lead to the prevention of any improvements to health care and in pharmaceuticals that could be achieved through research. If the health sector could not get access to information about the effectiveness or otherwise of drugs, they would instead have to rely on information obtained from pharmaceutical companies.

5. Two further problems with confidentiality identified were that the 'public interest' aspect of confidentiality could vary widely and it was difficult for people to assess what was in the public interest, while it was also difficult to assess what people's expectation of confidentiality was when they provided information. Again this could widely vary - some for people, for example, would assume that their data was not going to be shared with anyone other that their doctor.

A culture of fear

6. In local government, one member of the group suggested that there had been a growth in expectation that agencies would work closer together and the so the sharing of data had to be greater and more effective. However, there was a lack of confidence in local government about what could be shared under the Data Protection Act. This was also partly due to a lack of clear authority to share data and a fear that contravention of the DPA could lead to punishment. This view was wrong, as in actual fact there had been very few data protection-related sanctions meted out against local government, but it was a commonly held view and led to an overly-cautious approach to sharing data.

7. Front-line practitioners were worried about contravening the Act; by adverse reports in the media about data losses etc; and about losing control of the data they held. This was inhibiting the development and provision of public services.

8. This fear also existed in the health sector, according to one attendee, and was coupled with a culture of inertia, where it was viewed as being easier to not have to assess whether data could be shared or not. They felt that this may have be a result of the Hippocratic Oath, which had caused a culture of 'not sharing must be right' to develop. Statutory duties to share may override some of this fear and inertia, but legislation was often not the way as it could add to the confusion and was not an appropriate route to follow where the data could already be lawfully shared and where better guidance and training was a better solution.

<u>'The Solution'</u>

9. One attendee felt that there needed to be a much clearer distinction between the issues surrounding data sharing and data use for public protection with using data for public service provision.

10. Another attendee suggested that a National Information Governance Board be established that would approve Codes of Practice for specific data sharing initiatives.

However, questions were raised about how such a Board would tie into the work of the Information Commissioner's Office.

11. What was clear, according to one attendee, was that better, more authoritative guidance was required. The perception is that at present there was a mess of guidance on data sharing, and practitioners did not know which piece of guidance was the one they should be following. Generally, guidance focused on data protection, and stopping data being lost or misused, rather than what could be done under the DPA. People needed guidance on what could be shared for the provision of public provision without unacceptable intrusions of privacy occurring.

12. One attendee suggested that there was a case for raising technical expertise, particularly on the use of Privacy Enhancing Techniques, within organisations that used data. Another member of the group agreed, suggesting that trusted areas (or 'safe havens') should be established which employed vetted and trained staff who could when it was permissible to share data and how to share that information, e.g. anonymised, pseudonymised, under strict safeguards etc., and that the Office for National Statistics' 'virtual microlabs' could be the prototype for this type of centre. However, it was noted that the quality and type of PETs available varied greatly. Having a central point of expertise for the use of PETs could help but it would need to avoid becoming a regulation function.

13. Many of those attending the workshop called for greater clarity of what we meant by 'sharing', with some calling for some kind of taxonomy of data sharing. The term needed to be 'unpacked', and explained in a plain-English fashion. One attendee suggested that a clear, concise statement or principles of what could be done under the terms of the Data Protection Act needed to be produced, specifically to further the provision of public services and with the focus on what you could do, not what you can't.

Workshop 4 - 20 March 2008

Attendees

Anna Fielder, National Consumer Council
Bernard Baker, Intellect
David Townend, The University of Maastricht
Harry Cayton, National Information Governance Board for Health and Social Care
Mark Turnbull, Leeds City Council
Professor Dame Joan Higgins, Patient Information Advisory Group
Professor Martyn Thomas, Institution of Engineering and Technology
Rob Carmichael, Intellect
Steve Pennant, London Connect Limited
Sureyya Cansoy, Intellect

Introductions

1. It was explained at the outset of the meeting that the discussion would form part of a series of workshop sessions designed to feed into the evidence being gathered by the Data Sharing Review. The objective of the workshop was said to be to give those

present an opportunity to set out and discuss views and ideas on the use and sharing of personal information, including the context and method; the benefits and risks for society and the individual; and possible changes to current law and policy. In terms of structure, it was proposed that the first hour of discussion should focus on 'the problem' (i.e. is there anything within the current framework of law/policy/practice that causes concern, and if so, what is it?); while the second hour of discussion should focus on 'the solutions' (i.e. how can we remedy anything that is thought to be a problem?).

2. At the beginning of the discussion, two very broad points were made about data handling generally:

   i. It is important to strike a clear balance between rights and responsibilities. In this regard, and focusing on responsibilities, you can draw an analogy between the Health and Safety sphere and the information sphere - whereas in the former, individuals/organisations are robustly held accountable where they negligently cause damage/injury to people, in the latter that is not always the case. It was suggested that individuals could and should rightly be held accountable where they cause loss or damage in an information context because, first, they are in a position to remedy the problem; and, second, they are morally responsible for having caused the loss in the first place. However the Health and Safety analogy was not quite as easy at it seemed - when handling information you are necessarily faced with subjective judgment calls and it is difficult to produce systems with failsafe mechanisms if you are reliant on human beings making decisions. It was added that an illustration of the value we place on personal data is found in the need to prove financial loss in order to be able to claim compensation for data breach - surely if privacy is worth something, compensation should be paid for a breach of privacy *per se*.

   ii. There are certain questions which are important to ask as a first step when you consider issues around data handling/sharing/security. Importantly, one should look at the particular context of the data and ask what the data is, why it was gathered and how it was gathered. The answers to those questions will then determine the measures that are appropriate for the handling etc. A 'one size fits all' approach will not work. For example, in the healthcare sector, issues surrounding data are likely to be personally sensitive and so sharing data would have to be considered within that context. Other sectors will have different sensitivities and so judgement calls could be slanted in different ways. One attendee strongly supported this view, citing the National Consumer Council report, *Consumer Futures*, which found a growing divide between well-educated customers, who are comfortable e.g. using the internet for transactions and who understand about hidden costs such as bank charges; and poorer families, who find it impossible to work their way through glitches with bills and labyrinthine telephone complaints lines. Different people would have different information needs and so context was all-important.

‘The Problem’

3. Subsequent discussion fell under particular themes.

Balancing ‘benefits’ and ‘harms’

4. One attendee was keen to see the possible risks and harms associated with data sharing articulated more clearly. They suggested that forms of harm that could be suffered as a result of personal data sharing included data loss leading to ID theft and fraud (so financial loss and/or inconvenience to the victim). But they suggested that the key harm was discrimination - personal information being mishandled so that it falls into the hands of an unauthorised/inappropriate third party who then uses the information to discriminate against the data subject. It was suggested that, particularly where a data subject is unaware of what their personal information is being used for/how it is being used, discrimination could easily lead to social exclusion.

5. On the treatment of individuals by organisations, one member of the group suggested that discrimination based on an interpretation of personal information was often commonplace. They cited as an example the practice of High Street banks to ‘profile’ their customers - banks would routinely treat the student differently to the ‘City’ professional. In the public sector, another attendee suggested that the free school meals scheme was an example of where individuals were distinguished by raw personal data and then treated differently as a result (broadly, discrimination).

Privacy and the ‘Facebook generation’

6. It was noted that it was often assumed that people who had done nothing wrong should have no legitimate reason to hide information and so privacy should not be accorded any particular importance over and above other rights. But one person felt such assumptions were plainly wrong - for example cases involving the location of adopted children necessarily demand that personal details should not be widely available (if a natural parent tracked down the child, particularly where the child was young, very difficult emotional problems could result); and similarly cases involving the victims of domestic violence (where the victim and any children s/he may have will need to be kept safe from the perpetrator) illustrate a legitimate need to hide. There were many other examples too. However, the concept of privacy was being undermined by e.g. the social networking etc culture, where the younger generations are signing away rights without any real ‘informed’ consent/understanding.

7. Another group member said that younger people were all too often posting details about their lives (including embarrassing photographs/stories), which could be accessed by such a huge pool of people, including (years down the line) their own children, grandchildren or employers. One attendee explained that information posted on social networking sites could be stored for years into the future, irrespective of whether you as an individual account user decide to delete your

account at some point - information will continue to be held and could be reused/processed in the future without your knowledge. This point was supported by another attendee who felt that although children and young people are posting ever more personal information on the internet, it is not true to say they are consenting (at least in any meaningful way) to website owners taking their personal data and then reusing them. They drew attention to another NCC Report, *Fair Game*, which focused on these issues. Another attendee said that the questionable consent issue went further than young people - whenever e.g. people buy new software applications they are required to 'tick the box' agreeing with the standard terms and conditions, which include data processing clauses, but this is not to say that those people read, understand or agree to the terms.

8. One member felt that it is difficult to predict what the fallout from the 'Facebook revolution' will be. For example, in a generation's time, it might be the case that people can only become successful celebrities if they have embarrassing photographs of their youth posted on the internet.

Public sector culture

9. One attendee said that the public sector, as a general rule, was not good managing personal information. They suggested that technical capability was often considered before looking at business benefits against the backdrop of a Privacy Impact Assessment. Another person said that trust in the Government/public sector's ability to manage citizens' personal information was low. While individuals might trust e.g. social networking/e-commerce websites with their personal data, examples of public sector incompetence (like the data discs lost by HM Revenue & Customs) or in transparent practices (like the Driver and Vehicle Licensing Agency (DVLA) *selling* people's information to private car clamping companies with very little scrutiny as to whether there was a justifiable case for the information being supplied) gave people very little confidence in the State. One member of the group suggested that all too often the Government shot itself in the foot in the context of information management. They cited as an example the DVLA television advertising campaign that includes a 'if you don't pay your car tax, we know where you live' message, saying that the 'Big Brother' connotations were not helpful in a climate where Government/the public sector is not widely recognised as trustworthy in managing personal data.

10. One member of the group commented on the health sector. They suggested that data sharing in the National Health Service (NHS) tended to be driven by the benefits likely to accrue for the organisation and/or those working within it; rather than being designed to yield tangible benefits for data subjects themselves. The information culture of the NHS is illustrated well by the organisation's management of personal data - if a patient wants to ask the NHS what personal information is held on him/her, the NHS in all likelihood will either not want to give the information, or just will not be able to give the information. It was suggested that the NHS could not tell you how many databases it owned. But there was no excuse - it was possible to search e.g. over the internet for second hand books and seek data matches for the book of your choice against around 3 million

different datasets. Functionality like this would be extremely beneficial in reversing people's perceptions of NHS/public sector information handling.

11. In the welfare/benefits context, people applying for benefits face a process that is needlessly complicated and which often requires duplicate information to be provided for each separate benefit claim. One member suggested that the system's complexity was not only a hindrance for claimants (the very people the system was designed to protect) but that it also meant that auditing the system was necessarily complicated and so fraud could be relatively difficult to uncover. On a more positive note, they mentioned the Department for Children, Schools and Families' *Contact Point* initiative, which will deliver a database to be used by practitioners to find out who else is working with the same child or young person - the basic idea is that children's personal data are largely not accessible through the database but instead you can find appropriate contacts from whom relevant information about the child in question can be obtained, so making it easier to deliver more coordinated support. However, the speaker added that the issues around Contact Point were controversial and that the model was perhaps not yet ready to be held up as an example of good practice. In particular, focusing on the 'trust' issue, they said that it would be interesting to see whether Government would be willing to surrender all the information contained in the database once the children become adults.

12. Another attendee said that the workshop presentation slide ["So what is the problem? (3)"] articulated very clearly the problems faced by local authorities. In particular, neither legislation nor practice were keeping pace with the growth in data sharing capability; too many people were uncertain about whether or not they could share in particular circumstances and much of the guidance was useless; beneficial data sharing at local service-level was being frustrated by risk adverse centralised rules and by popular distrust of central government; and accountability was becoming less clear in a complex data sharing environment. It was suggested that, as a result of these problems, vulnerable children were not being protected as they should and local authorities were not achieving the efficiency possibilities they should be and that although the Information Commissioner thinks that he has insufficient powers, he is probably the "scariest figure" in local government: local authority employees are worried about falling foul of 'the rules' and as a result are overly risk adverse.

Power of the State

13. There was a discussion on how far the State should collect and use information on citizens. With one attendee stating that Government's efforts to establish massive databases (e.g. nation ID card scheme) were misconceived: where a large resource exists with potentially valuable information, people will try to hack in and break it because they stand to gain. Instead, local/federated systems were much more sensible. Another person said that Government had failed to lead the way on sensible and beneficial data sharing arrangements across the public sector. However, another saw nothing wrong with collecting information in one place and specifically advocated the creation of a national ID database, so long as risks to security etc were managed

appropriately. The proliferation of separate national unique identifiers from different Government Departments was not at all sensible. But they suggested that ensuring that citizens "own" their information would perhaps be a better solution to the 'power of the State' issue. Individual citizens could own and manage their personal information and allow different parts of government to access relevant information as they (the citizens) thought appropriate. Citizens could also update any information as/when necessary. Keeping information in one place is technically possible and central storage could then allow appropriate information to percolate across the government sector, helping e.g. services to improve. It was noted that giving individual citizens complete control over all their information could give rise to problems as e.g. official sanction is required when you want to change your name - allowing people to update their own names as they wanted would clearly not work.

14. Another person made the point that policy in the United Kingdom was based on the premise that people don't exist by permission of the Government, but that the Government exists by permission of the people. So citizens should not have to justify their existence to the State, nor should they have to justify where they go or what they do, so long as they are committing no crime(s) whilst doing it. That being the case, one member of the group said that they would object e.g. to the security services trawling systems that show where they had travelled on their Oyster Card - the objection was not because they had something to hide, but that they had nothing to hide and it was no one else's business. MI5 might have legitimate cause to trawl records in response to a terrorist attack (or ahead of a suspected attack) or serious crime - but all depended on the definition of "serious crime". In conclusion, they did not necessarily object to all access to information by the State but any such access to personal information should be tested rigorously on each occasion to ensure it was transparent, legitimate and fair.

15. One attendee suggested that the appropriate test that a State organisation should meet when seeking access to shared data was whether it is resourced to follow-up on the information it receives; and whether in fact it will follow-up on that information. So e.g. if the Police receive information from traffic cameras and from DVLA that shows drivers on the road without tax, will the Police follow-up *all* drivers identified as having broken the law? If not, then the quantity of information being sought from the camera operators/DVLA is clearly the disproportionate, and the use of the information would be potentially discriminatory (if e.g. only certain individuals were followed-up with further investigation). So if a public good is being claimed from data sharing, then the organisation should have to establish that the public good will, in fact, be realised.

16. Picking up on the proportionality theme, one attendee felt that although it was legitimate e.g. for Transport for London (TfL) to use data on people's journeys in order to plan more effectively, there was no reason why TfL needed to know the identity of each of those people for that planning purpose. HC said that he refused to register for a TfL Oyster Card online because he would have to provide his personal

details. But another person liked the online system because it suited their needs - which highlighted that these things always come down to personal choice.

17. For one attendee the information management culture in the UK was very different to that e.g. on continental Europe, citing Belgium as an example. In Belgium, the State operates a national ID card system linked in with biometric passports. But citizens do not fear the system, nor do they campaign against it. First, the ID card is complimented by a web-based 'portal' system, where citizens can log-in and see details of who has been looking at their information, and what they have used it for. Second, the ID card is seen as an 'enabler': it is not sold as e.g. an anti-terror device where the all-powerful State holds information to 'protect' individuals, which gives rise to lots of 'Big Brother' connotations. There was also an optional under-18 ID card, which young people can use to protect themselves e.g. in internet chatrooms. One attendee agreed that the culture in continental Europe was very different to that in the UK. The Scandinavian countries, for example, were very open with information sharing. And lots of countries have good systems and processes that protect personal information. But they were more optimistic than those that proclaim doom and gloom in the UK: feeling that the rate of change in both technology and culture will mean people look back in five or ten years time and wonder what all the fuss was about.

18. It was suggested by one member of the group that MI5 having access to information like Oyster Card records was necessary but being too transparent about it simply added to a climate of fear - he asked why people had to know what data the security services were using if it was used in the public interest. But another attendee said that the 'terror' tag often used by the Government was a red herring: there are few if any examples of data protection rules that inhibit law enforcement agencies doing what is necessary because they already have wide exemptions from e.g. the Data Protection Act. And picking up on the Oyster card discussion, someone else suggested that if the State has the power to track terrorists via their travel cards, then terrorists will just change to travelling by cash. So vast powers will end up meaning access only to information on the law-abiding majority. Another person added that many of the powers being requested are said to be "in the public interest": but who defines 'public interest'? If it is the State, surely what it means is in the State's interest, which may not necessarily meet the interests of citizens.

<u>'The Solution'</u>

19. It was suggested that the focus of the discussion should shift to considering the 'solutions' to the problems identified, and in particular to focus on what, if any, specific recommendations could be made by the Data Sharing Review when it reports. Various suggestions were made:

    i. One attendee noted that the Cabinet Office maintains the *Manual of Protective Security* (MPS), a document that contains general security requirements and guidance for the handling of protectively marked information and that they

understood that the MPS is used by contractors building e-systems for the Government, so that the e-systems built will meet the necessary security requirements. However, the MPS is not open to public scrutiny as it is marked 'classified', a marking the speaker thought was absurd. There were two reasons why the document should be made public, namely that it would be available for peer review to ensure its robustness; and that it could be used as a benchmark for accountability, so assuring the public that security guidelines were being met (or otherwise, as the case may be);

ii. A clear distinction should be made between *identification* and *authentication*: where all you need to prove is that you are entitled (or have the appropriate credentials) to access a service/buy a product, then it is unnecessary to prove who you are as well as that you have the relevant credentials - so for example it would be absurd to have to provide your name and address in order to buy a packet of cigarettes from a dispenser machine when all you should need to do is prove you are over the relevant minimum age;

iii. Statutory breach notification should be considered but that such a system should be backed-up by a statutory minimum level of compensation, immediately payable on breach. So, for example, if organisations were obliged to pay £10 to each person affected by a data breach for which they were responsible, those organisations would very quickly learn the value of personal data and you would be unlikely to find examples where the details of 25 million individuals are loaded onto data disks and then lost;

iv. It was stated that the concept of personal control over information was important and suggested that the 'data freezing' system developed and used in some U.S. States was worth considering - under this system, each individual is able to lock their credit reference file, unlocking it only when they want to use it (e.g. when applying for a loan). This is an anti-fraud device, which would make it extremely difficult for people to arrange credit using your identity. This idea was supported by another member of the group who suggested that this system could be extended beyond the Credit Reference Agency files to other sources of personal data, so ensuring individuals had real control;

v. One member felt that the Privacy Impact Assessment (PIA) was a very useful device, which should be used more often to allow properly thought out policy development. They suggested that PIAs should be carried out by independent auditors, not by the organisation seeking to benefit from the proposed policy;

vi. Another attendee supported the 'positive justification' principle outlined on the workshop slide ['Possible recommendations (1)'] - and suggested that anyone seeking to establish a case for sharing data should be obliged to show the benefits that are expected to accrue; should be obliged to follow-up on those expected benefits by trying to realise them; and if they do not follow up as they proposed, the right to share should then be withdrawn;

vii. They also suggested that the current Subject Access Rights (SARs) are not sufficient to allow people to access their own personal data easily enough. They cited access to General Practitioner medical records, saying that people found it very difficult to discover what personal information was held about them, and agreed that the *Health Space* website could potentially be used to help citizens access their information more effectively but he said that that functionality was not currently part of the design concept. Another attendee added that there would be some issues that needed to be resolved before something like *Health Space* could be used to divulge sensitive records. He cited a hypothetical example of a young Muslim woman in a sexual relationship with a man outside of her ethnic/religious group - if that girl fell pregnant but did not want her parents to find out, she could conceivably be forced to log-on to her online Health Space account by (and in front of) her parents, so allowing the details of her pregnancy to be known by them. In the most extreme cases, this could fall to be literally a life and death situation;

viii. For one member of the group issues around the process for registering data controllers could be looked at, specifically in the context of 'Prior Checking'. Under such a system, prospective data controllers will not be able to process data immediately upon registration (as is the general rule currently) but will require clearance from a supervisory body (the Information Commissioner's Office, or ICO) first. The ICO would need to be properly resourced if such a system were to be provided for;

ix. One attendee highlighted the importance of training and awareness. In the health sector, professionals' awareness was relatively good, particularly where health care professionals were working one-on-one with patients - and the Caldicott Guardians were a large part of the reason for this success. JH said that appropriate resources would have to be assigned in order to make any training/awareness programmes effective. Another person felt that guidance and awareness should be sector-specific, as so many issues/problems common to one particular sector are different in the contexts of other sectors. Another added that any training/guidance should focus not simply on data *protection* but also on data *sharing*, helping to show that sharing personal data could lead to real benefits, so long as the risks are appropriately managed. The concept of a Code of Practice was considered to be useful, but one member of the group encouraged the Review not to focus on separate code*s* of practice - a problem with the current regime is that guidance is too disparate, which does nothing to help inform people on the ground. The idea of a single 'framework' code was sensible, setting out the core principles across the board, which can then be added to by sector-specific guidance as/where appropriate;

x. When writing its report, one attendee said that the Data Sharing Review should not feel constrained by technology - just because the Review might assume something is technically impossible does not necessarily mean that it is. The Review should espouse the core principles as it sees them and throw the challenge to the market

of developing electronic and other systems that enable those principles to be realised;

xi. A particular focus for the Review should be the export of personal data - data being moved outside of the UK/EEA is not afforded protection under national or European law, and the voluntary agreements in place supposedly to cope with this issue simply do not work. One person made the point that, with the ever-increasing rise of global e-commerce, this issue was one that would become steadily more important;

xii. One person suggested that the Data Protection Act's second principle[2] could be amended so as to mirror more closely the intended effect of the European Directive's Articles 10 and 11[3]. Another suggested that the Health and Safety environment could again be looked at, this time with regard to the 'Hazard Analysis' device and that the test of whether the second principle had been met was whether or not a Privacy Impact Assessment, drafted at the time when the personal data were first collected, would need to be changed. If not, then the re-use is clearly compatible with the original purpose - but if a change would be required, then the second principle test is not met; and

xiii. The Review was encouraged to take account of the research community when developing any recommendations for reform, saying that the issue of data management rules were of critical importance to the effectiveness of scientific and social research.

20. There was also a short discussion on the issue of consent, with one person saying that the concept of 'informed consent' was extremely important, drawing on earlier discussions around the tick box (take it or leave it/all or nothing) 'consent' typical with e.g. software packages. Another stated that the Department for Work and Pensions was developing the *Tell Us Once* (TUO) initiative, which aimed to take personal information and pass it on to other service provider public bodies in order to reduce the burden on citizens. They suggested that the team working on TUO must have considered issues around consent and so the Data Sharing Review might get some useful guidance from them and another made the point that the issue of consent could be looked at as something akin to a contractual relationship between citizen and service provider. If this analogy were to be accepted, it opened interesting questions like whether the Unfair Contract Terms Act 1977 could be applied, and so whether 'consent' provisions deemed unfair under the Act could be challenged.

21. The discussion session closed when each participant was given the opportunity to mention one specific change that they would like the Review to consider as a

[2] Data Protection Act 1998, c29, Schedule 1, Part I paragraph 2: "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".
[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

recommendation when it (the Review) comes to report. The following suggestions were made:

- The Review should not feel constrained by assumed current technological capabilities [see paragraph 19 (j) above];

- There should be more of a culture where individuals 'owned' their own personal data [see paragraph 19 (d) above];

- The importance of the training and awareness points made during the workshop was reiterated [see paragraph 19 (i) above];

- There should be more statutory and enforceable guidance, as opposed to the many and various non-binding guides currently available;

- Another reiterated the importance of the context of the information in determining what measures are appropriate in managing the data [see paragraph 2 (b) above];

- The State should invest as a priority in a strategic programme to develop robust internet security systems to enable the potential benefits of public sector data sharing to accrue in an environment where risk is much reduced -the technology available today (particularly the off-the-shelf technology, and even today's on-line banking technology) was relatively easy to work around if you put your mind to it, e.g. through phising/spyware/virus attacks. But it was possible to improve e-security and it was within the resources of the State (as opposed to private individuals of firms) to develop that technological capability;

- One attendee emphasised the value of transparency and control, saying that neither existed to a sufficiently high degree in the current climate of data management;

- The potential benefits that could accrue from 'prior checking' was reiterated[see paragraph 19 (h) above]; and

- The Review was encouraged to focus on the needs of citizens, not organisations, and in particular at the interests of the vulnerable.

Workshop 5 - 25 March 2008

Attendees

Alan Cranston, Department for Children, Schools and Families
Becky Hogge, The Open Rights Group
Dave Wright, Eurim
Dr Leonard Anderson, Logicterm Ltd

Dr Tony Calland, British Medical Association (Wales)
Guy Herbert, NO2ID
John Harrison, Edentity Ltd
Nick Partridge, Terence Higgins Trust
Phil Booth, NO2ID
Professor Sir Michael Rawlins, National Institute for Health and Clinical Excellence
Rob Navarro, Sapior Ltd
Toby Stevens, Enterprise Privacy Group Ltd

Introductions

1. The group were informed of the background to the review and the purpose of the workshop meeting - to identify what problems existed with the current data sharing and data protection regimes in the UK, and the possible solutions to those problems.

'The Problem'

2. For one attendee the Government was clearly determined to do even more data sharing (as demonstrated by the Department of Constitutional Affairs data sharing vision statement and the recent Transformational Services Agreement), and there was a danger that the Data Sharing Review could be hijacked by the political agenda and used as a pretext for allowing the Government to use and share more personal information. In addition, the review appeared to be looking at the issue from a utilitarian perspective by viewing privacy as something to be traded off against the benefits of sharing data.

3. This view was backed by a member of the group who felt that the business case for sharing data was not always clear, with the Government in particular guilty of confusing the benefits for them with the benefits to the individual - even though the risks associated with data sharing would fall on the individual. It was highlighted that the Government was also confused between the sharing personal information and the use of aggregated data. Another attendee also felt that data sharing should only take place when there was an 'absolute benefit' for the individual in doing so, e.g. a person's medical records available to doctors in any part of the country they are receiving treatment. Societal benefits could also be realised through the use of aggregated data to track the effectiveness of drugs etc, but this should only take place on the basis of absolute, clear and informed consent.

4. Technology was highlighted as a factor in furthering Government's desire to share data, but without proper infrastructures, designed around the citizen, in place. There was a tendency in Government to avoid difficult technical developments due to a culture of risk aversion. In one attendee's opinion, the Government needed to recognise the importance of protecting data and having proper security measures in place, but privacy pressure groups also needed to recognise the benefits for the individual and society through the effective sharing of personal information.

5. However, for some members of the workshop, the possible benefits that might be realised could not be used to justify data sharing generally. The risks involved needed to be analysed at the individual level, and the worst case scenarios should not be downplayed simply because they wouldn't affect the vast majority of people.

6. The Government was seen as being under more greater pressure to do ‘more with less’, leading to pressure on Government to manage its resources better, including information. Retaining access to information was also linked to retaining trust from people and Government therefore needed to show it was capable of protecting data coupled with greater transparency of how and why it used information. Building on the theme of trust, one respondent used the example of people who were HIV positive having their medical records used in research. Many HIV patients could see the benefit in doctors and researchers having access to this information as it could lead to better treatments for them, but they were also deeply worried about such sensitive information being inappropriately disclosed. Trust in having this information suitably protected is therefore of the utmost importance, and the level of trust a patient has will effect whether a patient is more open or more restrictive about who has access to their health records.

7. People needed to have trust in the security protecting their information, and there had been a perception, particularly in the public sector, that data sharing could be ‘done on the cheap’, something which was demonstrated in the large amount of data breaches which occurred due to corners being cut. When data was lost a lack of means or incentive for the market to rectify itself was also identified as a problem, with little incentives in place for organisations to protect themselves against breaches. In this vein, one member noted that the Government could not have a mandate to change the private sector unless it had its own house in order.

8. Accuracy of data was also seen as a problem. People may enter information onto systems in different ways, e.g. listing chest pain as angina, which could then make future use/diagnosis difficult. Those providing data should have a duty to ensure that the data they provide is accurate.

9. The issue of consent was raised and whether it was ever truly informed. People generally had a lack of understanding of how much sharing actually took place (e.g. the general ignorance surrounding the selling of DVLA data to private car parking firms): the amount of data available, who could access it and who could share it. This lack of understanding could lead to inappropriate use of consent as a basis for sharing information. One attendee felt that it should be recognised that personal data is owned by the individual, and how it is used should be more transparent, with greater individual control.

10. Consent was highlighted s being a particularly problematic in the research arena, and it was not seen as a helpful basis for using information, as the refusal of consent could skew any results leading to inaccurate results. However, wherever possible, the majority of respondents felt that consent should be sought. Sometimes this wouldn’t be possible due to the high costs and time pressures involved, but new technologies could be employed to allow individuals greater control over how their information is used and by whom. Consent structures would take a long time to develop, but electronic access to data by individuals would make seeking consent easier and cheaper. myHealthSpace was a good example of such technological solutions, but investment had been lacking in user-centric technologies.

‘The Solution’

11. The subject of debate then moved on to what possible solutions could be found to the above problems, or to have a better regime in place for the use and handling of personal information.

12. One attendee felt that regulation was not the solution - the ICO was already overloaded and even if funded to the same level as the Health and Safety Executive it wouldn’t be able to monitor all data sharing activities. Part of the solution was giving individuals rights that they could exercise; otherwise there was little that could be done to control major companies using their personal information. Data sharing could happen two ways, either where everything took place in ‘the back office’ and the individual doesn’t have to do anything, or where the individual controls what is shared between multiple organisations, but designing systems that were more citizen-centric was seen by many of those attending as being the best way forward.

13. Sound risk based approaches to data sharing were called for with the benefits for any information sharing being demonstrable within a set timeframe, while many attendees felt that all data sharing schemes must be shown to be proportionate. One example put forward was ContactPoint which one attendee felt was disproportionate as their understanding of it was that it would list details of every child in the country when in an attempt to protect children at risk of harm, when in reality only 1% of the country’s children would be in an at risk group.

14. Data breach notification legislation was also put forward as a possible solution, as was the need for greater transparency and accountability. However, one respondent cautioned against data breach notifications, feeling that a glut of organisations washing their dirty linen in public would make people become immune to such announcements and the need to protect personal information. One member of the group suggested that a value needed to be created for data and become part of an organisations balance sheet. People working with personal information would then soon learn to properly protect personal information.

Workshop 6 - 31 March 2008

Attendees

Alex Markham, Connecting for Health
Bill McCluggage Office of the First Minister and Deputy First Minister
Bill Peace, Serious Organised Crime Agency
Carol Dezateux, Medical Research Council
Clare Jennings, NSPCC
David Carter, GB Group
Dr Eric Metcalfe, Justice
Elena Crasta, Trade Union Congress
Giles Watkins, Ernst & Young LLP
Gillian Key-Vice, Experian
Gordon Wanless, NHS
Hannah Reed, Trade Union Congress
Jill Kirby, Centre for Policy Studies

Karen Pile Department for Business, Enterprise and Regulatory Reform
Ms Alexis Cleveland, Transformational Government, Cabinet Office
Natalie Ceeney, The National Archive
Professor Chris Bellamy, Nottingham Trent University
Rob Laurence, GB Group
Roger Styles, Central Sponsor for Information Assurance, Cabinet Office
Susan Daley, Symantec

Introductions

1. It was explained at the outset of the meeting that the discussion would form part of a series of workshop sessions designed to feed into the evidence being gathered by the Data Sharing Review. The objective of the workshop was said to be to discuss views and ideas on the use and sharing of personal information, focusing on 'the problem' (i.e. is there anything within the current framework of law/policy/practice that causes concern, and if so, what is it?); and 'the solutions' (i.e. how can we remedy anything that is thought to be a problem?).

'The Problem'

2. The discussion opened with member of the group asking what it was we meant by 'sharing'. Do we mean sharing data horizontally, across departments, within organisations etc? For them, the problem was that the issues of data handling and protection had started from a 'silo view' that had created a restrictive regime under the Data Protection Act - in service delivery, most of the time you just wanted to know if, for example, someone was eligible to receive a benefit, where a 'yes' or 'no' answer would suffice. But you might need to share data to do this, and the DPA could prevent this from happening.

3. Another attendee agreed that the 2nd Data Protection Principle (DPP) of the DPA (data must not be used for purposes incompatible to those for which the data was originally collected) could hinder data sharing for beneficial reasons from occurring. This was because the wording of the 2nd DPP was unclear, and deciding whether any data sharing was compatible with the 2nd DPP was something that even lawyers could often not agree on. Establishing whether a body had the *vires*, or power, to share data was also difficult where there was a mix of statutory and crown bodies, and in their opinion having a statutory footing for sharing data was a better route to follow than relying on common law powers.

4. One person agreed with this last point, suggesting that the health sector often had no need to know a person's identity, but that uncertainty over what data was permissible to access and share under the law had created a culture of risk aversion. Another attendee noted that data was not homogenous and that for one area, such as the health sector, a piece of information may not be as important as it would be to another area, such as law enforcement. The importance of data was, therefore, in 'the eye of the beholder'.

5. It was suggested that people did not really care about how their data was used, only the results they get as a result, e.g. access to finance and credit, or when something goes wrong. Even if tools designed to create more transparency about data use are

used, e.g. Fair Processing notices, and are used well, people will rarely look at them. However, others felt that if people had greater understanding of what data sharing occurred they might be more concerned about keeping their data secure, which in turn would have a knock on effect on organisations using data - investing more effort in keeping data secure to meet a customer demand.

6. One person attending the workshop had conducted some research into front-line practitioners' attitudes to using and handling data. This indicated that the law wasn't seen as being the real problem for people when deciding to share information. People were more concerned that if they shared the information they have collected, then it would be more difficult to collect data in the future as individuals would be less 'honest' in the information they provide - e.g. drug abusers may be less willing to be honest with social services if they think the information will be passed to the police.

7. For some members of the group, the perceived push towards greater data sharing, particularly by Government, was a worrying development. Having Government departments working in silos, for example, was not necessarily a bad thing - they could act as safe havens for data and offer more safeguards. If Government wanted to follow the programme of Transformational Government, then the public should have an opportunity to decide whether they wanted to withdraw or engage with the subsequent data transactions that would take place between different parts of the public sector, particularly, as opposed to the private sector, people did not have a choice about whether to use a public service or not.

8. One attendee stated that data was a commodity for the business of Government, and that there was a huge obligation on the Government to protect and assure this information. However, Government did need to carry on sharing data if the benefits of creating joined-up services were worthwhile. If they were, then Government must have the right technologies, processes, and people in place to share data safely and proportionately.

9. There was agreement that having the right people in place to decide whether to share data or not and then handle the process effectively was vital. One person felt that there had tended to be too much focus on using regulation to ensure data was handled correctly when the focus should be on the people handling the data. Another member of the group favoured keeping a light touch, principles based regulatory framework, coupled with greater education, training and assessment of those people making judgements around personal information. As a member of the group had noted, data sharing could not be viewed in an abstract way, it occurred for varied reasons and was carried out by a range of people and organisations. It would therefore be impossible to legislate for every possible scenario, and there were currently not enough carrots to encourage better data protection - only penalties for getting it wrong.

10. Not sharing data, it was pointed, could be equally damaging as sharing data, e.g. the lack of information being shared between police forces that allowed Ian Huntley to get a job in a school in Soham. Data may not be shared for a number of reasons, often because of confusion about what could be done, or a fear of getting into trouble for releasing information inappropriately, but there could also be genuine, real rather than perceived, barriers that prevented data sharing for beneficial purposes from occurring. The voluntary sector was, for example, unable to access information it

needed to properly fulfil obligations Government placed on them, even when the information was actually held by Government. In one example cited, this was because the relevant Government department in question did not have the *vires*, or legal power, to share the information.

11. Another problem identified, was a general lack of leadership in the privacy/data sharing debate, particularly from Government. The argument usually leans towards a defensive reaction to things going wrong, such as the Government announcing reviews when the headlines are bad. What was needed was a positive, forward-looking discussion on the positives of sharing data in a proportionate, safe and sensible way, and that avoided knee-jerk reactions that introduced a more risk adverse environment.

<u>'The Solution'</u>

12. The discussion the moved on to what could be done to improve the current operation of the Data Protection Act and the handling and sharing of personal information more generally. The following points were put forward for consideration.

13. Guidance and training were obviously key areas. Guidance on sharing data between different sectors and more guidance on the application of the 2nd Data Protection Principle were called for, and one attendee said they would like to see some sort of Highway Code for data sharing. Clarity over current guidance was also needed. A large number of bodies produced their own guidance (MOJ, PIAG, ICO, GMC, BMA) and people could get confused about what data to follow, so some sort of hierarchy of guidance could be useful. In terms of training, people needed to be empowered to make judgements, following a set process and without fear of recrimination or penalty if this process has been followed. Organisations which provide training should also be encouraged to design and run courses on data handling and data sharing, perhaps backed up by a recognised set of qualifications.

14. People making judgements about data sharing should be accredited and there should be clear audit trails for how decisions were reached. Lines of responsibility also needed to be transparent. Organisations data sharing arrangements should be open to scrutiny and challenge by the public, with one member of the group suggesting that some form of standard template should be created for Government to use to inform people about what data Government uses, who it shares it with and why.

15. One person suggested that data breach legislation should be introduced, whereby companies had to inform their customers if they lost any of their data. They cited research carried out in America [where such legislation exists in many states] that indicated that the consumer felt a greater sense of empowerment when informed of breaches as it allowed them to control and protect their information themselves. However, some attendees felt this could overly burden companies, and data breach notification legislation, in one attendee's opinion, could lead to stigmatisation, distress or impossible situations to resolve - e.g. a National Insurance number would be impossible to change, so what would be the point of telling someone this information had been 'lost'?

16. Another attendee felt that it was important to be more realistic about the benefits that data sharing could bring, and there were many examples of expensive data sharing projects that had failed to achieve what they intended to do. Technology should be used to give individuals greater control over their own information, and Government should move away from large databases and data sharing projects that occurred with little interaction with the individual. This would help to maintain trust between the public and Government, something Government would need if it wished to push ahead with the Transformational Government agenda. Another attendee agreed that people should be given a degree of control over how information about them was used. But sometimes this needed to be overridden.

Workshop 7 - 3 April 2008

Attendees

Alistair Maughan, Morrison & Foerster LLP
Christopher Rees, Herbert Smith LLP
Dr Ian Brown, University of Oxford
Eduardo Ustaran, Field Fisher Waterhouse LLP
Ian Lloyd, University of Strathclyde
Paula Barrett, Eversheds
Professor Douwe Korff, London Metropolitan University
Richard Jones, Clifford Chance LLP
Rosemary Jay, Pinsent Mason
Ruth Boardman, Bird & Bird
Serena Hardy, Ministry of Justice

Introductions

1. It was explained at the outset of the meeting that the discussion would form part of a series of workshop sessions designed to feed into the evidence being gathered by the Data Sharing Review. The objective of this legal-specific workshop was said to be to give those experts present an opportunity to set out and discuss views and ideas, in particular on the future development of the legal regime governing the use and sharing of personal information. The discussion would be most useful in the context of the Data Sharing Review if attendees focused both on any perceived *problems* and on potential *solutions* to those problems.

Framing the debate

2. One attendee stated that they hoped the workshop discussion would focus on high-level issues - most importantly on privacy as an important human right - rather than on lower-level technical details, which could simply serve to confuse the 'bigger picture'. As part of setting the scene for that high-level debate, they questioned whether it was correct to use as a starting point (as he suggested the Government do) the premise that information sharing is a good thing in itself. Another attendee agreed, saying that the starting point should be individual and personal autonomy within a context geared to protecting human rights: that is the fundamental

constitutional approach that should be adopted for data sharing issues. They added that the issues involved far more than a simple balancing exercise: to share any information an organisations needs to establish that it would be acting within the law (including with the law of the European Convention on Human Rights and the European Directive on the protection of personal data); and that the sharing was necessary (not merely preferable).

3. Another member of the group expressed surprise at the tenor of the debate thus far. Although they agreed that there was an important constitutional right to privacy, they also said that individuals now have to accept that they are living in a modern global economy that demands at least some information sharing. In that context, they suggested that it would be more useful to design a system with robust and effective regulation to ensure that the sharing that does take place is fair, rather than seeking to prevent potentially beneficial data sharing on the basis of ideology. Another attendee agreed, saying that data sharing now occurred on a massive and global scale each and every day. Every click on the internet can be monitored by Internet Service Providers, and that (almost) every step could be monitored by CCTV - everyone should get used to that. They suggested that the focus should be on creating a regime that would protect individuals' privacy as far as possible; but one that would also facilitate necessary and beneficial data sharing where appropriate. The current regime inhibited legitimate and potentially beneficial information exchange in some instances. As an example, the *Sure Start* initiative was cited, which it was suggested needed access to data on certain families in order to help target services and help at them, but found it very difficult to obtain that information.

4. One attendee rejected the contention that the present system acted as a barrier to beneficial data sharing, saying that in their experience they could not point to a single example of legitimate data sharing being prevented by the law, suggesting that it would be important to define an agreed set of values and standards in the field of information management. In particular, they suggested that it would be important for the Government to develop (and then stick to) broad principles, encompassing all the positive and beneficial protections afforded by international law. However, another person said that examples like the Soham murders and the 7/7 London bombings illustrated a need for law enforcement and security agencies to share information in certain circumstances and so the debate should be broader than simply one about individual privacy.

Consent

5. It was suggested that the concept of 'consent' was becoming meaningless in the modern data processing world. As an example of this, one person cited their journey to the workshop, which involved a flight from Strathclyde to Gatwick. During the flight and, so far as they were aware, without any prior notification, domestic passengers were told that they would have their photographs taken on landing. The airline were clearly collecting personal information (the photos) but that there was no opportunity for genuine 'consent' from the passengers, nor for passengers to find out why the

information was necessary and what use(s) it would/could be put to - so consent and transparency were lacking, although just guaranteeing transparency did not mean that the consent problem would be solved. They added that, where data sharing did take place, it was becoming increasingly difficult to determine who the allocated data controller was at any given point, and so ultimately who bore responsibility for protecting the data.

6. A number of those present agreed that the way in which 'consent' is understood is becoming confused, and that there was often a "misbadging of consent". The basic point was that 'consent' is only an appropriate term where the data subject has a genuine opportunity to make an informed choice. So where companies purport to seek consent from customers before e.g. granting a licence to use computer software, or before issuing a credit card, consent cannot be genuine because there is no real choice: either you agree to the standard terms or you can not access the service. One person said that different sectors operated in different ways, with e.g. the health sector tending to treat 'consent' with appropriate respect. The motivation of the health sector was probably more related to the law of confidence rather than the Data Protection Act, so focusing only on amendments to the Act would not address the mischief.

7. Another member noted that, as the Working party established under Article 29 of the EC Directive concluded, consent was not always an appropriate way to legitimise data sharing. If there is a public need to share information irrespective of the wishes of individual data subjects, then it could clearly be beneficial for that information to be shared. But they added that, in any circumstances where consent was not appropriate, there should be a clear *legislative* statement authorising the proposed sharing exercise. They would express the general rule as being consent should always be required, save for where legislation identifies a clear public imperative for the data to be shared.

8. Another person suggested, however, that attempting to assign an overly significant value to consent would be to slow down the processing of information, to the detriment of public services and commercial practices. Rather than focusing on consent as a perceived protection for individuals, it would be better to improve privacy management techniques, including data minimisation and the (perhaps compulsory) use of Privacy Impact Assessments (PIAs).

Sanctions

9. One attendee stated that the regulatory regime that currently exists provides nothing to make them advise their clients: "you really must do this or it will hit you in the pocket". Another person suggested that even the threat of reputational damage is something that organisations are becoming immune to. Without tougher sanctions in place, they added, it would remain difficult to convince people to comply with the rules and take data protection seriously.

10. Another person agreed that the increasing number of data breaches was in effect desensitising the public and organisations to the damage that can be caused by the misuse of personal information. They therefore agreed that some more effective form of sanction or remedy would be beneficial. However, another attendee was sceptical about the extent to which the law (and in particular, the criminal law) could effect societal/attitudinal change and suggested that what was more important was empowering consumers/data subjects through, e.g. affording them greater protection against cost orders in the courts and in particular making it much more difficult to be bankrupted as an individual claimant; allowing litigants in person to appear in more informal (tribunal/small claims) hearings, so avoiding additional and unnecessary legal costs; and/or removing the necessity to prove quantifiable loss/damage in order to bring a claim (instead making the defendant organisation liable for a strict liability fixed-penalty charge in cases where they were shown to have breached the law). They felt that each of these suggestions would facilitate the bringing of civil litigation suits against organisations, which should in turn force those organisations to 'up their game' and improve the protection afforded to individuals' personal data.

The DPA's fitness for purpose

11. At this point it was suggested that the tenor of the debate so far could be summarised thus far by saying that some sort of regulatory or sanction-based change could be beneficial but that no one had identified any more significant problems with the way that the current regime operated. Attendees were asked whether it was correct that, save for some focus on additional sanctions, the Data Protection Act 1998 (DPA), as it currently stood, was sufficient to deal with modern information management/data sharing; or whether some more substantial changed was required.

12. Broadly speaking, everyone agreed with the basic proposition that the system was not in need of radical overhaul. For example, one attendee said that they and their clients liked the principles-based approach of the DPA as it was not too prescriptive or restrictive. Another member agreed that increased sanctions could be beneficial, suggesting that many firms in the financial sector were "scared" of the FSA's regulatory powers, and this helped maintain high standards throughout the industry. The suggestions for change were made:

    - Although there was a need to ensure appropriate protection for individuals' personal data, there was also a problem in facilitating necessary/ beneficial data sharing under the current regime and so four potential solutions were suggested namely: (a) the Information Commissioner's Office producing a binding Code of Practice to *enable* (not *restrict*) data sharing; (b) introducing some 'carrot' into the system to ensure that high data protection standards are maintained, including e.g. consideration of mandatory Privacy Impact Assessments, or perhaps tax-breaks for organisations that voluntarily use PIAs; (c) providing the ICO with stronger auditing powers, like in some other jurisdictions; and (d) focusing far

more on ensuring transparency of data management (including sharing) practices;

- It was also suggested that the market could be used to help take some pressure off the ICO in regulating all data management practices across the board. As in Germany, the regulator could certify private sector e-products (e.g. privacy systems) as compliant with the law and then offer incentives for organisations to use those certified systems in the market place. That way, the market would ensure that problems were kept to a minimum and the ICO could focus exclusively on the real problem areas. Secondly, the DPA was defective in implementing international law, in particular the EC Directive, and therefore the DPA should be amended. As an example, there was a discrepancy between Schedule 3 of the Act and Article 8 (3) of the Directive: whereas Schedule 3 paragraph 8 explicitly allowed processing of sensitive personal information for "medical purposes" including "medical research", the Directive did not extend so far as to include medical research. Moreover, it was also suggested that the ICO, not the Ministry of Justice, should be responsible for domestic legislation's compliance with international (including EC and ECHR) law, in order to ensure a more robust system of individual protection and legal compliance; and

- One member of the group highlighted a recent report[4] from the UK Parliament's Joint Committee on Human Rights, citing with approval the Committee's concern about the use of legislative 'gateways' for enabling data sharing. Their particular concern was with the powers that primary legislation often gives to secondary legislation to bring about (or change) gateways. In their opinion secondary legislation was no protection against the excessive Government action, since it is extremely rare than any secondary legislation is ever blocked and that data sharing should be dealt with by primary legislation, where real Parliamentary oversight can be guaranteed.

13. There were some suggestions that the DPA was "behind the times", particularly with regard to technological advancement, with one person submitting that that the DPA was developed before the more recent explosion in e-capabilities, meaning that the protections are now perhaps out of date. It was suggested that the DPA was perceived as having been drafted with Mainframe computers in mind, rather than digital technology in the internet age. However, another person said it "baffles" them when people suggest the DPA is outdated. As a technologist, they could see nothing that the Act could not cope with. Even powerful State organisations (including American intelligence and security agencies) could not read encrypted data and so no new level of protection against this threat was needed, whether in the DPA or elsewhere.

[4] The Joint Committee on Human Rights' 14th Report of 2007/8: Data protections and Human Rights. See: http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

The Second Principle

14. There was a wide-ranging discussion on the DPA's second principle[5] and whether it was fit for purpose. The following points were made:

- One person could not understand what the second principle was for, suggesting that, if they had their way, they would get rid of it altogether;

- Another suggested that the concept of a 'finality principle' was theoretically sound but that the current second principle seemed defective insofar as it was unclear how the test of compatibility (or 'not incompatibility') could be met, in particular because the vague concept could be interpreted in a very broad or a very narrow way. However, they agreed that it was impossible to decide whether or not information should be shared unless you know the purpose for which the information is required. The key should be proportionality;

- The second principle, one person suggested, was all about applying the concept of compatibility to data subjects' expectations, in order to protect those individuals and that PIAs would be a useful tool in this regard;

- For another member of the group the finality principle was useful but it was only one of the eight principles, and of no more or less validity/worth than the others, nor more important than international law. Insofar as the 'compatibility' issue was concerned, they suggested that the appropriate test should be whether or not the reasonable data subject would understand the subsequent processing as compatible with the original purpose;

- One attendee said that the requirement for purpose specification was a substantial aid to systemic transparency but that the drafting of the DPA's second principle (with the double-negative "not incompatible") was unclear and badly drafted. They also queried whether an effective mechanism to police compliance was in place, saying that the burden of reviewing all instances of information processing in accordance with each of the principles would be far too much for the ICO to cope with; and

- One person said that the second principle encapsulated what they described as the "British sense of fair play". The principle is aimed simply at ensuring common sense prevails in a system at which the consumer is at the heart (e.g. a patient would expect a doctor to share information for the purposes of treatment, but not in order to furnish a pharmaceuticals company with research data in return for profit) and that therefore it is a beneficial concept to retain in the legal framework. They were of the view not only that the second principle was sound, but that the principle-based approach of the DPA was sound, and that it required no (or no significant) change.

[5] DPA Sch 1, para 2: "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

Anonymisation and Pseudonymisation

15. There was a brief discussion on pseudonymisation, starting with the point that the device was used often where researchers would have no interest in the actual identity of data subjects but would need to be able to treat each separate data subject as a distinct individual to ensure e.g. no double counting, so standard anonymisation techniques would be insufficient in this regard. Attendees were asked for views on the protections that would need to be afforded where data is anonymised or pseudonymised.

16. The clear consensus was that full anonymisation was an appropriate device so long as there was no reasonable *likelihood* (or no unacceptable *risk*) of the data being 'de-anonymised', although one person said that the process of anonymisation would itself constitute processing of personal data and so the protections afforded by the DPA and other law would need to be observed fully. But another person highlighted this as illustrative of the mess that the data protection law can sometimes get itself into: why should doctors have to seek consent from patients before anonymising personal data and then using that completely untraceable information for other purposes?

17. Opinion was less clear-cut in terms of pseudonymised data, with three members of the group each arguing that there would need to be a genuinely powerful justification for using sensitive personal data for research purposes. One attendee pointed to Germany, where even the courts have limited powers to order disclosure of identities where pseudonymised data is concerned. And those that were less robust in this regard still argued against too liberal a stance, for example with another person suggesting that pseudonymised data should be treated sensitively and never e.g. posted on the internet, where others could access it and trace it back to original data subjects. It was also suggested that where information would be unlikely to be decoded, it should not constitute Personal Identifiable Information. In this context, somebody contrasted research under a clinical trial (where researchers would be actively unlikely to want to identify specific individuals involved) and internet-based advertising, where information about data subjects may be anonymised but where advertisers had a vested interested in discovering who each of the data subjects were, so making it more likely that actual identities would be traced. One member of the group felt that they would be prepared to allow pseudonymous data processing where the justification outweighed concerns about privacy.

18. The discussion session was drawn to a close when each participant was given the opportunity to mention one specific change that they would like the review to consider as a recommendation when it (the review) comes to report. The following suggestions were made:

- A reduction in complexity of the legal framework would be beneficial. The principles-based system under the DPA was good and that primary legislation should seek to go no further than establishing clear principles;

- One attendee cited the JCHR report on data protection and human rights and said that they would want the Review to take the protection of privacy seriously;

- Where problems exist in the current legal framework, they tend not to be focused on the DPA but on the wider law, and in particular on the law of confidentiality. That is therefore where any measures should be aimed, not at the DPA, which is performing well;

- Domestic law should ensure that it is in-line with European law, and that at the moment the former is falling short of the protections mandated by the latter;

- One person would not want to see the Review recommending anything that would be excessively prescriptive. Most people working in data management fields are "trying to do the right thing" and that the legal framework should help, not hinder them in that regard;

- Another person agreed that domestic law should ensure that it is in-step with European law;

- For one member of the Group the Review should recommend sanctions, including criminal liability for top executives (more analogous to the Health and Safety regime, where organisations really do understand and care about their legal obligations and responsibilities); and including heavier financial penalties (e.g. allowing the ICO to levy fines as a percentage of turnover to encourage the larger organisations to take the issues more seriously). They added that the fact Subject Access Rights (SARs) are so heavily used in the UK was an anomaly when compared to the rest of Europe - and suggested that the DPA section 7 rights should remain but that, if a data subject exercises those rights, s/he should be barred from using the resulting information to sue the data controller. They explained that they thought too many data subjects were erroneously using SARs as a collateral attempt to force documentary disclosure where litigation is pending, thus circumventing the usual processes of court procedure;

- One person would like to see notification/registration abolished unless the process is made more useful; mandatory PIAs; and more sector-specific statutory guidance on data management issues;

- Government should take a more principled stand on the protection of privacy, and that the principled stance should then dictate policy across the board in different Departments; and

- An appropriate balance was needed whereby sharing information was made as easy as possible through the issuing of clear guidance and e.g. Codes of Conduct from the ICO; and privacy protection is maximised as far as possible, with e.g. mandatory PIAs in appropriate circumstances.

Workshop 8 - 17 April 2008

Hosted and minuted by Intellect

1. Introduction to the government's data sharing review

In February 2008 Intellect submitted a response to the consultation on the use and sharing of personal information in the public and private sectors. The consultation will feed into the independent review on data sharing which, at the request of Gordon Brown, is being undertaken by Dr Walport and Richard Thomas, the Information Commissioner.

Intellect, in conjunction with the Data Sharing Review Team, hosted this industry workshop with the purpose of conveying the position of IT while the review is still in progress.

Dr Mark Walport led the discussion. Dr Walport is a Director of the Wellcome Trust and a member of the Council for Science and Technology, the Government's top-level independent advisory body on science and technology policy issues. The aim of this forum is to gain expert input on the technological aspects of many of the issues raised by the report so far.

2. Questions from the floor

-How does this review relate to Sir Gus O'Donnell's Data-sharing review?

Sir Gus O'Donnell's review looks at central government data handling and the processes around it. This is much wider and looks at principles around the sharing of information across public and private sectors, from an intellectual as well as practical viewpoint

-Has this review looked at training the public officials in charge of data get about handling it?

The culture of data handling needs to be changed. There is certainly not enough understanding of the level of accountability needed in boardrooms on this subject, for instance in comparison to something like health and safety.

-Will your recommendations apply to government departments?

The rules and recommendations of this review will apply to both public and private organisations. The report team are conscious of the unease about how government has the power to bypass data-sharing laws, for example by changing department remits with statutory instruments, which mean databases are moved around. This will be taken into account when making recommendations.

-Are there examples of practices not keeping pace with conditions?

With the advent of web 2.0, and the corollary blurring of the line between data owner and data controller, there will undoubtedly be a need for a new test of 'appropriateness' on information sharing.

There is also a need to consider legal jurisdiction across the world. For example Google information on searches made in the UK by UK citizens is kept in the USA, where federal law enforcement agencies have rights of access and no obligation to disclose to us that they are using it.

New rules also need to be laid down regarding the mechanism by which a decision is taken as to when personal data is interchanged between the private and public sectors.

- How have you approached the distinction between personal and public information?
The aggregation of personal data to create public data is a relatively new phenomenon, driven by technological advances, and requires further scrutiny. For example, information on traffic flows is useful public information. But it can now be gathered by monitoring individual car locations and tracking areas of congestion. That utilisation of private information to create public information blurs the lines of what is and is not appropriate.

- Have you considered the idea of a trusted third party which releases information to those that need it when they need it?
This idea has been raised in previous consultations. There is a school of thought which says that the information is already out, and therefore it is not possible to 'lock it down.' In this case, we would like to use this forum to discuss what we can do to bring in greater transparency. Is the fact that the data is already out there necessarily a bad thing?

Credentialing mechanisms have also been considered, i.e. the issue of details from a 3rd party which has a time expiry limit on it. This continues the Digital Rights Management example.

Discussions should bear in mind the distinction between data and information. Regarding the issue of data breach notification requirements under law, there is a need to increase security, as well as consumers' and citizens' understanding of their rights and how to protect themselves.

3. Breakout sessions

Dr Walport outlined the objectives of the breakout sessions, and urged the groups to consider the following questions when discussing the issues presented.

- What can we recommend to the public and/or private sector which will make a difference to how information is handled?

- Can you craft the law in such a way that the subject of the information is also the 'owner', therefore companies with it are holders, not owners?

- Is there a technological way of notifying a citizen each time their information is used? Is a public disclosure requirement any time information is shared a feasible idea?

- Define the difference between identity and a component - a name is not an identity on its own, but together with other components can form an identity. At what point does the level of information available become dangerous?

- How to ensure accountability accompanies responsibility

- Is consent to one organisation using data suitable consent in a broader sense?

Group 1 breakout feedback

- Article 8 of the Human Rights Act provides the framework for when the state can share information without an individual's permission. An organisation's data-controller should have purview and accountability over all information it holds.

- The cost of making information access available to everyone would be prohibitive However, there are parallels in the Electoral Roll. Its information is transparent, although very few people actually bother to look it up. The fact that it is there, however, is a guarantor of transparent democracy.

- In its current guise, the Information Commissioner's Office is fair and reasonable, but lacks teeth. It is easy for people to run around the Data Protection Act and interpret it as they will. It should emulate the Health and Safety Executive.

  The Financial Services Authority has the power to fine organisations if information breach incidents come under their remit. The ICO should hold the position of a regulator with the power to fine. It could also act as a sort of umpire as to whether what a company is doing with data is defensible in the public domain

- Organisations should keep a record internally of what personal information they hold on any individual, and the 3rd parties with whom they share it. Transparency is the key for the data subject. It would be augmented if technology could track what and to whom information is disclosed. Auditing of accounts about data would allow for application of responsibility. Publishing data protection officer and data controller appointments would aid accountability

- Additionally, there should be professional qualifications for those in charge of data protection. They should hold positions in their organisations equivalent to board level.

The following four key principles were identified as being crucial to informing future policy on data-sharing; Responsibility, Accountability, Consent, Informed decision making.

Group 2

This group discussed the following general points around the issue of data-sharing.

a) General

- Future proofing is essential - consideration needs to be taken around liability. Technology companies will in the future be asked to share information that wasn't specified in their initial service contracts
- Tesco is an example of a private organisation that collects and analyses much information for commercial purposes. The company takes strong measures to ensure the security of the information and as such is able to use it without much objection

b) Recommendations/suggestions for improvement

- A system/application/service that allows you to view all of your personal information held by agencies and organisations
- A shift in obligation - it would be beneficial to place the obligation on the data-holder to inform the data subject when their information is accessed and by whom (for example credit record holders)
- Ownership - currently there is no ownership of databases. To encourage greater concern for personal information, there must be more top down responsibility. For example, in Spain organisations are obliged to undertake rigorous measures to safeguard personal information
- There must be consideration of what information and data is available for whom - there was agreement that, for example, personal information detailed on birth certificates should not be publicly available
- Binary - binary answers to information requests are acceptable in many cases and negate the risk of sensitive personal information being divulged. Systems could be made to enable binary answers to information requests e.g. when verifying whether Emily is 18, the application/system should return a yes or no answer without divulging unnecessary personal information (dates of birth etc). Much the same is true for other examples in the insurance and credit areas for example

- <u>An Information Repository</u>
- A data holder - a trusted organisation who acts as a repository for personal information (similarly to the function Paypal executes with money)
- Lock down an individual identity until there is sanction to release personal information
- Authorisation for certain levels of information would be pre-defined
- “Pyramids” of information - access restrictions set enabling individuals to specify which agencies/organisations which levels of information. There was some concern that the user-centric concept of central data holder would not work as some individuals would not adjust ownership/sharing properties
- A trusted information repository could be a service provided by anyone who meets necessary standards

c) Standards/Legislation

- Data protection principles are adequate but are not reinforced by adequate enforcement legislation to ensure organisations and agencies comply
    - Power of inspection
    - Questioning of necessity - does a company really need certain data sets (e.g. data requested in forms - mother’s maiden name for passwords, details of spouse etc)
    - Powers of audit for information processes
- Standards are required to ensure that fines and sanctions are placed on organisations that lose personal data - required standards should be equally applicable to both the private and public sectors

d) Education

- MI5/Oyster Cards - attendees agreed with the concept of analysing data to reveal patterns of behaviour. As such, there is now a need to educate customers about the implications of certain technological advances and about the information age in general.
- Objections to sharing information lessen when people have an understanding of the benefits that that it will bring to them. There will need to be incentives for people to submit to their information being shared.
- ID Cards - attendees highlighted the scheme as an example of government not voicing well the issues around information, identity and entitlement. The terrorism argument does not convince individuals as the majority of people are not directly affected by it, whereas a piece around the efficiency gains that could be brought by the card/joined-up services would resonate with the majority of users
- An educational piece with very basic arguments about how recording, disseminating and maintaining information correctly will make life easier - crime stories should only form a minimal, background argument.
- Explain to people clearly that if their personal information is shared, it will make life easier e.g. if you tick a box on your passport form your photograph will be duplicated and used for any driving licence applications - this must be explained simply and clearly.

e) The Internet and Personal Information

- The Data Protection Act is flawed because of the proliferation of the internet. There may need to be a move to place more responsibility on ISPs - however, there is only so much an ISP can do to prevent the misuse of personal information and individuals should be reminded that they are personally responsible for their own information.
- It was noted that there are a limited number of locations identified as sources of child porn and that if the ISPs were to work together these sources could be shut down relatively quickly. Attendees thought that although a difficult area (ISPs are often outside jurisdiction of legislation) government should not be deterred from making a move towards legislating.

Group 3

a) General comments on Private Sector and Public Activity

- For whatever recommendations are made and procedures implemented, it was felt that complete transparency was absolutely vital.
- The public sector has an unfair advantage over the private sector in that governments don't need to get CESG clearance for data sharing.
- It would very useful to have universal standardised technical requirements, which spanned both the public and private sector.
- Access to data should be role-based.

b) Communication

- Consent to share data is often a requirement as opposed to a choice, and citizens should be informed well in advance of their options.
    - There is a huge amount of potential for technology to improve consumer understanding of data sharing issues and options (no specific solutions proposed)
- The Belgian ID card is an example where citizens are aware of what data the government holds, and what is being done with said data.
- It's necessary to instil a cultural change within the public sector; thus, it's vital to train public sector workers on the importance of data protection and data-sharing protocol.

c) Accountability

- Leadership issues
    - There was a need to make leadership more accountable, i.e. if proper measures were not instituted and followed, there would be substantial penalties.
    - Should a higher level of staff be responsible for making data-related decisions?
    - Should data sharing standards be determined and implemented at the local government level or the central government level?
        - As the term 'standard' can carry a negative connotation, it was noted that a different term would be better employed, e.g. 'best practice guidelines' or 'guiding principles'.
- It was thought that a regular information audit across government departments would be useful.
- Accountability standards would need to offer both sticks and carrots
    - Punishment should be meted out according to the level of seriousness of a data breach.
    - Benefits could also be offered for data sharing, e.g. the BS-7799 standard on information security management systems. Otherwise there could be incentives for industry to maximise its potential as a 'value-added secure agent' (e.g. through US Data Breach Notification Act)
- If corporate liability is considered an option, the Review Board would need to consider the ramifications of over-compensatory regulation, such as the Sarbanes-Oxley Act (SOX)

d) Commoditisation of data

- There was a fair amount of discussion around this theme, and it was suggested that if individuals were given ownership of their Personally Identifiable Information (PII), they would value it more.
    - Technology could aid this endeavour by developing an automated compliance process, which could allow individuals to either directly control their data or give consent to share data in certain instances.
- If citizens are given additional rights to control their PII, they should also have the corresponding duty of keeping their data up to date.

    - A government social networking site containing all the information held on a particular person would be one solution to helping individuals monitor their data.
- Ideally, individuals would be able to dictate to organisations on what they could do with individual data, but it was thought that this might be too difficult to implement.
- If new data about a certain individual is generated by a company, to whom does it belong? To the person the data refers to, or to the company that generates it?
    - This leads to a rationale for shared ownership of data between individuals and companies/government.

e) Future proofing

- The Data Sharing Review's notion of being able to implement a solution that would be valid for 15 years was thought to be unrealistic. **The consensus was that the Review Board should plan for constant renewal, and thus any framework that is instituted should be technology neutral** (as any technology adopted would likely be obsolete, or at least less efficient, after 5 years)
- There was a discussion around the merits of centralised databases, and opinion was extremely divided over whether central or local databases would prove to be more efficient.
- Globalisation-related concerns
    - Are standards within the UK enough? Should the UK and/or EU be pushing for global standards on data sharing?
    - The Review Board needs to consider the fact that any standards that are imposed within the UK may affect companies' activities abroad, and hinder their international competitiveness.

4. Summary

So far there has been a demonstrable benefit in the sharing of data - sharing data well can make money for an organisation or increase its efficiency etc. This is the 'carrot' but there is still no real 'stick'. There has also been a failure on the part of government to adequately explain the benefits of information sharing to citizens, which needs to change if we are to embrace and utilise to best effect the technological and social developments which surround it. The outcomes of this consultation will be considered along with the rest of the work done towards this report, and will undoubtedly provide a helpful technological insight into the practicality of many of the suggestions being made so far.

Annex E - Bibliography

1. *A surveillance society?*, House of Commons Home Affairs Committee, 2008
2. *Better use of personal information: opportunities and risks*, Council for Science and Technology, 2005
3. *CCTV code of practice*, Information Commissioner's Office, revised edition 2008
4. *Challenges and opportunities in identity assurance*, Sir James Crosby
5. *Data handling procedures in Government: Final Report*, Cabinet Office, 2008
6. *Data Protection and Human Rights*, Joint Committee on Human Rights, 2008
7. *Data Protection Law and Practice*, Rosemary Jay, Sweet & Maxwell 2007
8. *Data Security in Financial Services: Firms' controls to prevent data loss by their employees and third-party* suppliers, Financial Services Authority, 2008
9. *Digital healthcare: the impact of information and communication technologies on health and healthcare*, The Royal Society, 2006
10. *Directors' Guides to Managing Information Risk*, Neil Robinson, Information Assurance Advisory Council, 2008
11. *fair game?: Assessing commercial activity on children's favourite websites and online environments*, National Consumer Council, 2006
12. *Freedom of information: Government's proposals for reform*, House of Commons Constitutional Affairs Committee, 2007
13. *FYI: The new politics of personal information*, Peter Bradwell and Niamh Gallagher, Demos, 2007
14. *Information Commissioner's Office: Annual Report 2006/07*
15. *Information Sharing Protocols Position Paper*, EURIM Personal Identity and Data Sharing Group, 2008
16. *New Dimensions in Privacy Law: International and comparative perspectives*, edited by Andrew T. Kenyon & Megan Richardson, Cambridge University Press, 2006
17. *Overlooked: Surveillance and personal privacy in modern Britain*, Gareth Crossman et al, Liberty, 2007
18. *Personal Data for Public Good: Using health information in medical* research, The Academy of Medical Sciences, 2006
19. *Privacy and data-sharing: The way forward for public services*, Performance and innovation Unit, 2002
20. *Privacy Law in Australia*, Carolyn Doyle & Mirko Bagaric, The Federation Press, 2005
21. *Protecting Government Information: Independent review of Government information assurance*, Nick Coleman, Cabinet Office, 2007
22. *Protection of Private Data*, House of Commons Justice Committee, 2008
23. *Report of the Committee on Data Protection (Lindop)*, Her Majesty's Stationery Office, 1978
24. *Report of the Committee on Privacy (Younger)*, Her Majesty's Stationery Office, 1972

25. *Report on the review of patient-identifiable information*, The Caldicott Committee, Department of Health, 1997
26. *Research Report Fair Processing Notifications: Current Effectiveness and Opportunities for Improvement*, Corporate Solutions Consulting (UK) Ltd, Information Commissioner's Office, 2007
27. *Review of information security at HM Revenue and Customs: Final Report*, Kieron Poynter, 2008
28. *The British Computer Society: Celebrating 50 years*, John Kavanagh, The British Computer Society, 2007
29. *The forensic use of bioinformation: ethical issues*, Nuffield Council on Bioethics, 2007
30. *The Future of Privacy: Volume 1 Private life and public policy*, Perri 6, Demos, 1998
31. *The Future of Privacy: Volume 2 Public trust in the use of private information*, Perri 6 et al, Demos, 1998
32. *The Glass Consumer*, Suzanne Lace et al, Policy Press, National Consumer Council, 2005
33. *The Governance of Privacy: Policy instruments in global perspective*, Colin J Bennett and Charles D Raab, MIT Press, 2006
34. *The Impact of Surveillance and Data Collection*, evidence submitted to House of Lords Constitution Committee inquiry
35. *Treading Water: The 2007 technology, media & telecommunications security survey*, Deloitte, 2007
36. *What price privacy? The unlawful trade in confidential personal information*, Information Commissioner's Office, The Stationery Office, 2006
37. *Who Knows: Safeguarding your privacy in a networked world,* Ann Cavoukian and Don Tapscott, Random House Canada, 1995
38. *Working document on the processing of personal data relating to health in electronic health records*, Article 29 Data Protection Working Party, 2007
39. *Working Document on the protection of children's personal data,* Article 29 Data Protection Working Party, 2008

Annex F - ICO suggestions for change and clarification of the Data Protection Act

1. Personal Data

The Data Protection Act 1998 has been in force for over ten years. However, despite court and Information Tribunal rulings, and guidance from the Information Commissioner, there remains considerable uncertainty as to the precise scope of the DPA. A significant area of uncertainty concerns 'border-line' personal data. By this we mean information that may not constitute personal data according to a strict reading of the DPA's definition, but which could be linked fairly easily to other information to form personal data. Another significant area of uncertainty concerns the DPA's application to non-computerised personal information, i.e. information recorded as part of a 'relevant filing system'.

2. Border-line personal data.

It seems to be fairly well understood that the DPA applies to records that explicitly identify individuals - their tax returns, health records and credit reference files, for example. However, the situation is far less clear in the case of information that does not explicitly identify individuals, for example by naming them, but which could be combined fairly easily with other information to allow explicit identification to take place. For example, the addresses of a company's members of staff, without their names, does not constitute personal data according to a strict reading the DPA. However, the addresses could be combined fairly easily with other information, for example the electoral roll and information on the organisation's website, to allow particular staff members' addresses to be determined. Given this, a sensible approach would be for the organisation to treat its staff members' addresses as if they did constitute personal data, for example by keeping them secure and guarding against their improper disclosure. However, as it stands, the addresses do not constitute personal data and the DPA provides no protection to the individuals concerned. We do not think that this should be the case. We believe that apparently subtle differences between the European Data Protection Directive and the DPA have led to significant legal uncertainty and have undermined the protection that the Directive was intended to afford to individuals in border-line cases.

The concept of identification that lies at the heart of both the European Directive and the DPA may always prove difficult to apply in practice. However, in our opinion the definition of personal data in the Directive has certain advantages over the one found in the DPA, particularly in the context of 'border-line' personal data. In the UK legislation, personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. The Directive says that 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The problem concerning the scope of the UK legislation emanates primarily from the reference to 'the data controller' in the definition of personal data. The use of "the" strongly implies that we are talking of identification being carried out by one party; the 'primary' data controller. However, we do not think that this is the intention of the Directive. Recital 26 of the Directive gives guidance on how to determine whether a

person is identifiable. It makes it clear that for the purposes of the Directive, in order to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. The approach to identification taken in the Directive is, in our opinion, easier to apply in practice, clearer and deals more realistically with the issues of identity that organisations and individuals are increasingly facing. It provides more meaningful protection to individuals in the context of a society where it is becoming increasingly easy to share, analyse and combine data sets. There is a strong argument for replacing the definition of personal data found in the DPA with that contained in the Directive.

The issue of identification touches on a deeper problem concerning the application of data protection law. As it stands, data protection is an all or nothing concept. If information constitutes personal data, then the entire data protection system of principles, responsibilities and rights must apply to it. In the medium to long term, there is a strong case for a much more flexible application of data protection law. For example, in European data protection circles the view generally prevails that IP addresses held by internet search engines constitute personal data. Assuming this is the case, then individuals should have a right of access to the IP addresses that support their internet search sessions, and, some argue, individuals' consent should be obtained to process IP addresses. However, search engines have no means of identifying individuals explicitly. They cannot name them, contact them or take any action in respect of them; the most they can do is individuate one internet searcher from another. However, IP addresses could be combined with other information, typically that held by an Internet Service Provider, and ultimately this could lead to the real world identification of an internet searcher. Therefore, in our opinion, data protection law's principles of transparency and security ought to apply to IP addresses because they have the potential to form personal data. However, it makes no sense in practice to expect the right of subject access, for example, to apply to the information. A more flexible, componential approach to the application of data protection law would also work well in respect of other sorts of information, for example CCTV footage of individuals who have not been identified, but ultimately could be, for example if the footage is analysed and combined with eye-witness statements and other intelligence as part of a police investigation.

3. Relevant filing systems.

The definition of 'relevant filing system' has caused significant legal uncertainty and practical difficulty for individuals and data controllers since the DPA came into force. Judgements in the courts have done little to clarify which collections of manual information fall within the scope of the DPA, and which records the data protection principles, and rights such as subject access, apply to.

The Directive defines a 'personal data filing system' as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. Recitals 15 and 27 clarify that the Directive only covers manual filing systems whose content is structured in a way that allows easy access to personal data. Recital 27 also makes it clear that files or sets of files which are not structured according to specific criteria shall under no circumstances fall within the scope of the Directive.

The DPA defines a 'relevant filing system' as any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is

structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Though there remains considerable room for debate about the proper interpretation of this definition, it is quite clear that the intention was that it should be construed narrowly.

In our opinion the most useful approach to the definition of 'relevant filing system' is a purposive one. Put simply, we believe that if a file is structured in such a way that it is of practical use to an employer, for example, in finding out certain information about an employee, then the rights and protections provided by data protection law ought to apply to that file. It is clear from debate during the reading of the Data Protection Bill that the government favoured a definition that would only apply to highly structured collections of information, replicating the sub-divided tree-structure of computerised information. It was argued at the time that even a fairly short personnel file, within which it was in practice very easy to locate a particular type of information about an employee, for example his or her attendance record, should not be covered by the DPA. This approach, and the adoption of the DPA's definition, means that the test of whether the DPA applies to a particular file rests on tortuous consideration of matters of structure, rather than on how a file can be used in practice. In our opinion this is against the spirit of the Directive.

In our opinion the principles of data protection should apply to records, like personnel files, whose content can have such a significant effect on individuals, and where the inaccuracy or loss of information could cause such detriment. Record holders should be under a duty to ensure that personnel files, and similarly significant records, are kept accurate and up to date, even if they are not highly structured. In our opinion, substituting the Directive's definition of 'personal data filing system' for the DPA's definition of 'relevant filing system' would help to address the problems described above.

4. Discretion for the Information Commissioner not to carry out an assessment in every case.

When he is asked to do so, the Information Commissioner is required to carry out an assessment of whether it is likely or unlikely that the processing of personal data is being done in compliance with the DPA. The Commissioner enjoys a degree of flexibility in terms of the way he carries out an assessment, and has made great efforts to channel his resources towards the investigation of complaints where there is evidence that the processing of personal data has caused real problems for individuals. However, we can see advantages in providing a clear statutory basis for the Information Commissioner to decline to make an assessment, for example where the issue being complained about is trivial or inconsequential or where the complaint is frivolous or vexatious. This would allow more of the Commissioner's limited resources to be devoted to the investigation of significant complaints and to other forms of regulatory activity. It would also allow the Commissioner to put an end to the practice of making 'unverified assessments'. In these cases, an assessment is made without necessarily verifying the facts underlying the complaint or seeking the data controller's side of the story. We would very much prefer the Information Commissioner to be in a position where he investigates properly complaints that warrant investigation, but rejects outright complaints that do not. This is a model that some other European Data Protection Authorities have adopted, without any apparent problems in terms of their duty under the Directive to hear claims.

5. Better information gathering powers for the Information Commissioner.

The Information Commissioner's primary means of obtaining information in order to investigate a complaint, or to determine whether the data protection principles are being complied with, is to serve an Information Notice. As it stands, the Commissioner can only serve a Notice on 'the data controller'. This power may be sufficient in fairly straightforward cases where a single organisation is being complained about, or where the Commissioner wants to look at a particular organisation's information handling practices. However, the Commissioner increasingly deals with issues where a number of organisations, who may or may not be the data controllers, are jointly involved in an enterprise. In such cases it would be helpful if the Commissioner could serve an Information Notice on any person where he reasonably requires information to investigate a complaint, or to determine whether the data protection principles are being complied with. This is a power enjoyed by some other European data protection authorities, and which equates much better with the power for the Commissioner to collect all the information necessary for the performance of his duties, provided for by Art.28 of the Directive.

6. Confidentiality of Information.

Section 59 of the DPA subjects the Information Commissioner, his staff and former staff to a strict prohibition on the disclosure of information that relates to an identified or identifiable individual or business. We can see the need to ensure that members of Information Commissioner's Office, including the Information Commissioner himself, are bound by confidentiality rules. The individuals and businesses that the Information Commissioner deals with must have confidence that the information they provide to the Commissioner will not be disclosed without proper authority. Indeed, the Directive requires that members and staff of the supervisory authority are subject to a duty of professional secrecy. However, as it stands, s.59 of the Act applies not only to the Commissioner and his staff as individuals, but also to the Commissioner as a corporate entity. We believe that this causes uncertainty for ICO corporately, for example in terms of its need to demonstrate how it is using its powers and resources and how effective it is being. We suggest that s.59 goes against the principles of open government, public accountability and regulatory good practice. In our opinion s.59 of the Act should be amended to make it clear that the confidentiality of information arrangements do not apply to the Information Commissioner as a corporate entity, but only to the Commissioner and his current and former members of staff as individuals.

7. The right to seek compensation for distress alone.

As it stands, an individual is only entitled to compensation for a contravention of the DPA if distress and damage is suffered. We can certainly envisage cases where the loss or improper disclosure of a person's health record, for example, could cause an individual a degree of anxiety and concern that affects his or her life quite severely, but which does not amount to damage.

Section 13(2) of the DPA entitles individuals to compensation for distress caused by a contravention of the Act if the contravention relates to the processing of personal data for the journalistic, artistic or literary purposes. This clearly envisages the courts in the UK being able, in certain circumstances, to award compensation for distress without damage. Ultimately it's for the courts to decide whether distress can be of such a degree that it warrants compensation. However, in our opinion it would be consistent with the UK's obligations under the Directive for individuals to have an entitlement to compensation for distress alone, whether or not the special purposes are involved.

Annex G - ICO Framework Code of Practice

Framework code of practice for sharing personal information

Information Commissioner's foreword

Sharing information can bring many benefits. It can support more efficient, easier to access services. It can help to make sure that the vulnerable are given the protection they need, that organisations can cooperate to deliver the care that those with complex needs rely on. Law enforcement agencies must have access to the information they need to counter the increasingly sophisticated methods that fraudsters and other types of criminal are using. Our time is valuable. No one likes being asked to provide the same information over and over again. No one wants to discover that their doctor doesn't have access to relevant information about their health.
Sharing information presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people. There is a danger that the public will be left behind, subject to opaque information systems that they do not understand and that they have no control over. No one wants a huge database of personal information that anyone can access for any, ill-defined purpose.
This framework code of practice can be used in various ways in a variety of contexts. It contains simple, practical advice that will help all those involved in information sharing to develop the knowledge and confidence to make good quality decisions about sharing personal information. This framework code of practice will help to make sure that the benefits of information sharing are delivered, while maintaining public trust and respecting personal privacy.

Richard Thomas
Information Commissioner

About the framework code of practice

Why a framework code of practice?

The Information Commissioner's first statutory duty is to promote the following of good practice in the handling of personal information. 'Good practice' means practice that appears to the Commissioner to be desirable, having regard to the interests of individuals and the organisations that process personal information about them. Good practice includes, but is not limited to, compliance with the requirements of the Data Protection Act 1998 (the Act).
The Commissioner has produced this framework code to help organisations to adopt good practice when sharing information about people. The framework code is intended to be of use to all organisations involved in information sharing throughout the UK, including voluntary bodies. However, some of it will be of most relevance to public sector organisations. The framework code should be of use even where there is a statutory

requirement to share information. Using the framework code will help organisations to make sure that they address all the main data protection compliance issues that are likely to arise when sharing information. This in turn should help organisations and their staff to make well-informed decisions about sharing personal information.

The benefits of using the framework code of practice

The framework code breaks down compliance with a fairly complex piece of legislation into a series of logical steps. These should be easy for you to follow in practice, even if you're not a data protection expert. Organisations will face different compliance issues, and may adopt their own approaches to dealing with them. However, using the framework code should help organisations to develop a common understanding and a consistent approach.

Producing your own code of practice, and using it, will help you to establish good practice and to comply with the law. It will also help you to strike the balance between sharing personal information and protecting the people it's about. This should gain the trust of the public and make sure that they understand, and participate in, your information sharing initiatives. Following a good quality code of practice will also give your staff the confidence to make well informed decisions, reducing the considerable uncertainty that can surround information sharing.

Ultimately, following good practice should make your information sharing more effective, allowing better services to be provided to the public. It should also enhance the reputation of your organisation in the eyes of the people you keep information about.

What do we mean by 'information sharing'?

There are two main sorts of information sharing. The first involves two or more organisations sharing information between them. This could be done by giving access to each other's information systems or by setting up a separate shared database. This may lead to the specific disclosure of a limited amount of information on a one-off basis or the regular sharing of large amounts of information, for example bulk matching name and address information in two databases. The second involves the sharing of information between the various parts of a single organisation, for example between a local authority's various departments. The content of the framework code should be relevant to both types of information sharing.

The framework code is for use mainly in circumstances where information is being shared on a routine, systematic basis. However, in some cases information is shared in a more ad hoc way. For example, a teacher might use his or her professional judgement to decide to share information with a social worker because there is concern about a particular child's welfare. The framework code is not primarily intended for use in cases like that, although it may still be of use if read alongside the relevant professional guidance.

How to use the framework code of practice

Your organisation's needs

This framework code should be used by organisations that want to produce their own codes of practice for sharing information. It says what content a code of practice should have if it is to support good practice in the sharing of personal information. Organisations using the framework code must fill it in with their own detailed content, reflecting their own business needs. Where a number of organisations are working collaboratively on an information sharing project, it is important that any codes of practice do not contradict each other or overlap confusingly. In many cases it is best to have a single code of practice that all the organisations involved in the information sharing work to.
We recognise that different organisations have different needs, depending on the sort of information sharing they're involved in. We anticipate a considerable degree of flexibility in how the framework is used. For example, it can be used to produce a stand-alone document some or all of its content can be integrated into existing policies and procedures; or it can be used as a checklist to evaluate existing policies and procedures. We hope that the framework code will help organisations to design their own solutions to the compliance issues they face. However, the Information Commissioner's Office is willing to provide further advice and assistance when this is needed.

Endorsement

The Information Commissioner will endorse a code of practice based on the framework provided it addresses all its substantive content. For a code to be meaningful it must be adhered to in practice. To provide an endorsement we would normally expect an organisation to agree to us auditing compliance with its code.

The framework code and compliance with the law

Drawing up a code and following its recommendations in practice cannot guarantee compliance with the Data Protection Act 1998. However, adhering to a properly drafted code of practice would be a significant step towards achieving compliance with the Act. Each part of the framework code begins with a clear statement of what the Act requires. However, some of the content of the framework code goes beyond the strict legal requirements of the law. We have done this as part of our statutory duty to promote good practice in the handling of personal information. The legal requirement is to comply with the law. No action can be taken over a failure to adopt good practice or to act on the recommendations of the framework code.

Code of practice recommended content: 1. Deciding to share personal information

The law

Any information sharing must be necessary. Any information shared must be relevant and not excessive.

Your code of practice should do the following

1. Set out why you want to share personal information and what benefits you expect to achieve.
2. Provide for a realistic appraisal of the likely effect of the sharing on the people the information is about, and of their likely reaction to it.
3. Give advice on finding alternatives to using personal information, for example using statistical information.
4. Describe the information that you need to share to achieve your objective and the organisations that need to be involved.
5. Outline the relevant legal provisions, that require or permit your organisation to share information, or prevent it from doing so.
6. Address any issues that might arise as the result of sharing confidential or sensitive information.
7. Say whether individuals' consent for information sharing is needed and, if so, how to obtain consent and what to do if consent is withheld.

Points to remember

1. Before you start sharing information you should decide and document the objective that it is meant to achieve. Only once you have done this can you address other data protection compliance issues, for example, deciding whether you need to share information in a personally identifiable form, or whether anonymised or statistical information would be enough.

   You should determine right at the beginning of a project who will be responsible for dealing with the various compliance issues that will arise. All the organisations involved will have some responsibility. However, the organisation that originally collected the information has the primary responsibility for making sure it is handled properly. In particular, that organisation must make sure that sharing its information will not cause real unfairness or unwarranted detriment to individuals.
2. This can be done by carrying out a 'privacy impact assessment'. This involves assessing any benefits that the information sharing might bring to society or individuals. It also involves assessing any negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. It should help to avoid or minimise the risk of any detriment being caused.
3. It is not justified to share information that identifies people when anonymised or statistical information could be used as an alternative. This sort of approach can protect personal privacy while still allowing organisations to carry out their functions. In some planning contexts, for example, it may only be necessary to use general demographic information about people living in certain areas, rather than identifiable individuals' names, addresses and dates of birth.

4. Only relevant information and the minimum necessary to achieve the objective may be shared. You should review your arrangements regularly to prevent the sharing of information that is not relevant to achieving your objective. Where you are sharing information internally, for example, within a local authority, the same considerations apply. If only certain departments are involved in providing the service that the information sharing is intended to support, only those departments should have access to the information.
5. Some organisations are required by law to share information for a particular purpose.

   In these cases you must be clear about what information you are required to share and in what circumstances. If you are unclear about this you should get legal advice. Other organisations are allowed to share information, for example, where this is necessary for a local authority to carry out its functions. In some cases an organisation may be expressly prohibited from sharing the information they hold. These organisations must be clear about the nature of any such prohibition. Again, if necessary, you should get legal advice about your powers.

   Many public sector organisations are bound by the European Convention on Human Rights. This means that any information sharing they carry out must be compatible with the convention, in particular the right to respect for private and family life. Organisations should also take into account any relevant professional guidance or industry code.

   You should regularly check your notification under the Act to make sure that it describes any organisations you are sharing information with.
6. The threshold for sharing confidential or sensitive information is generally higher than for sharing other forms of information. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals. Some information is so sensitive, for example that contained in a health record, that in normal circumstances a patient's explicit consent must be obtained if you want to share or use it for a non-medical purpose.
7. Sometimes data protection law only requires that the individual knows about the sharing of information, it is not always necessary to obtain his or her consent for this. However, if you decide that you do need consent to legitimise your processing of information, this must be a specific, informed and freely given agreement. In this context, a failure to object is not consent. Most importantly, the individual must understand what is being consented to and the consequences of giving or withholding consent. If you are relying on consent to share information about a person, you must stop doing so if consent expires or is withdrawn. You must be clear with members of the public about the role that consent plays in your information sharing.

   In this context, consent is not genuine unless its withdrawal leads to the information sharing being stopped.

2. Fairness and transparency

The law

Personal information shall be processed fairly. The processing won't be fair unless the person has, is provided with, or has readily available:

- information about your identity,
- information about the purpose the information will be processed for,
- and any other information necessary to enable the processing to be fair.

Your code of practice should do the following.

1. Give guidance on the drafting of 'Fair Processing Notices'.
2. Advise on ensuring notices are actively provided or, at least, freely available to the people you want to share information about.
3. Ensure that fair processing notices give a genuinely informative explanation of how information will be shared and that they are updated when necessary.
4. Provide for ways of dealing with requests for further information and enquiries from members of the public.
5. Help to ensure that explanations are given of the circumstances in which information may be shared without the individuals' knowledge or consent.

Points to remember

1. Fair processing notices, or 'privacy policies' as they are sometimes known, are intended to inform the people the information is about how it will be shared and what it will be used for. This means that a notice has to be drafted in a way that the people it's aimed at will understand. Drafting notices for children and others whose level of understanding may be relatively low requires particular care. You should avoid legalistic language and adopt a plain-English, easy-to-read approach. Ideally, your code of practice should contain examples of model fair processing notices.

   You must decide whether a single fair processing notice is enough to inform the public of all the information sharing that your organisation carries out. In some cases it would be good practice to produce a separate fair processing notice for a particular information sharing initiative. This would allow much more detailed and specific fair processing information to be provided. In other cases a more general notice could be enough. An existing notice may already explain all the information sharing you are engaged in. If this is the case, no further action is needed.

   2.A fair processing notice is meaningless unless people can read it and understand it. At least, you should make sure your fair processing notice is readily available. You should try proactively, though, to provide fair processing notices to people, for example when you hold meetings with them or send out a letter. You should normally provide fair processing information when you first obtain information about a person. Where you intend to share confidential or particularly sensitive information you should actively communicate your fair processing information.
3. Information sharing arrangements can be quite complicated, with different sorts of information being shared between various agencies. However, you have to give a comprehensive and accurate description of what information is being shared and who it's being shared with. An information sharing arrangement can change over time, for example where a public body is placed under a new statutory duty to share information to deal with a particular problem. This requires the public body to review its fair processing information regularly to make sure that it still provides an accurate description of the information sharing being carried out. It can be useful to adopt a 'layered' approach to providing fair processing information. This involves having a relatively simple explanation backed up by a more detailed version for people who want a more comprehensive explanation. This can be done fairly easily in on-line contexts.
4. Sometimes people will have questions about how information about them is being shared, or may object to this. It is good practice for organisations to have systems in place for dealing with enquiries about information sharing in a timely and helpful manner. The analysis of questions and complaints should help you to understand

public attitudes to the information sharing you're carrying out, and to make any necessary improvements.

5. There are cases where it is legitimate to share information without a person's knowledge or consent. This might be the case where a failure to share information about a parent's lifestyle would put a child at risk. There are also other situations where information should be shared despite a lack of consent, for example, where the sharing is necessary to safeguard public safety in an emergency situation. In many criminal justice contexts it is not feasible to get consent, because doing so may prejudice a particular investigation. However, you should be prepared to be open with the public about the sorts of circumstances in which you may share information without their knowledge or consent.

3. Information standards

The law

Information shall be adequate, relevant, not excessive, accurate and up to date.

Your code of practice should contain the following.

1. Procedures for checking that information is of good enough quality before it is shared.
2. Methods for making sure that shared information is recorded in a compatible format.
3. Procedures for making sure that any information that is being shared is relevant and not excessive.
4. Methods for checking regularly that shared information is of sufficient quality.
5. Methods for making sure that any problems with personal information, for example, inaccuracy, are also rectified by all the organisations that have received the information.

Points to remember

1. It is good practice to check the quality of the information before it is shared, otherwise inaccuracies and other problems will be spread across information systems. In general, any plan to share information should trigger action to make sure that inaccurate records are corrected, irrelevant ones weeded out, out-of-date ones updated and so on. It is not always possible to check the accuracy of every record: in these cases a sample of records should be checked. There should be mechanisms in place to help organisations to resolve problems where there is disagreement over an information quality issue. The exchange of information in paper form can cause particular problems. It can be very difficult to make sure that an organisation's collection of paper records is corrected once an inaccuracy is detected.
2. Different organisations may record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mismatched or becoming corrupted. Before sharing information you must make sure that the organisations involved have a common way of recording key information, for example by deciding on a standard format for recording people's names. If you cannot establish a common standard for recording information, you must develop a reliable means of converting the information.
3. Only once you have a clearly defined objective, for example the delivery of a particular service, can you make an informed decision about the information that is necessary to carry out that objective. You should be able to justify the sharing of each

item of information on the grounds that its sharing is necessary to achieve the objective. You must not share information if it is not necessary to do so. It is good practice to regularly review the information sharing and to check that all the information being shared is necessary for achieving your objective.

Any unnecessary sharing of information should cease. However, in some contexts it is impossible to determine with certainty whether it is necessary to share a particular piece of information. In these cases, you must rely on experience and professional judgement.

4. It is good practice to check from time to time whether the information being shared is of good enough quality. For example, a sample of records could be looked at to make sure the information contained in them is being kept up to date. It is a good idea to show the records to the people they are about so that the quality of information on them can be checked. Although this may only reveal deficiencies in a particular record, it could indicate wider systemic failure that can then be addressed.
5. The spreading of inaccurate information across a network can cause significant problems for individuals. If you discover that you have shared inaccurate information, you should not only correct your own records but make sure that the information is also corrected by others holding it. You need to have procedures in place for dealing with situations where there are disagreements between organisations about the accuracy of a record. In some cases, the best course of action might be to ask the individual whether his or her record is correct.

4. Retention of shared information

The law

Personal information shall not be kept for longer than is necessary.

Your code of practice should do the following.

1. Specify retention periods for the different types of information you hold, including retention times for the various items held within a record.
2. Provide for the regular review of retention periods, based on assessment of business need.
3. Set out any legal requirements or professional guidelines relevant to the retention or disposal of the information you hold.
4. Make sure that any out-of-date information that still needs to be retained but is not permanently deleted is safely archived or put ‘off-line’.
5. Specify whether information supplied by another organisation should be deleted or returned to its supplier.
6. Provide a mechanism for making sure that your retention procedures are being adhered to in practice.

Points to remember

1. Automated systems can be used to delete a specific piece of information after a pre-determined period. This facility is particularly useful where a large number of records of the same type are held.

   Considerations for judging retention periods include:

   - the current and future value of the information for the purpose for which it is held;
   - the costs, risks and liabilities associated with retaining the information; and

- the ease or difficulty of making sure the information remains accurate and up to date.

2. You should review your retention policy in the light of operational experience. If records that are being retained are not being used, this would call into question the need to retain them. It can be very difficult to assess the significance of the information you hold. In these cases you must rely on experience and professional expertise to come to a balanced decision about whether to retain or delete the information.
3. For example, there are various legal requirements and professional guidelines relating to the retention of health records. There may also be a legal requirement to keep an audit trail for a certain period of time.
4. There is a significant difference between permanently, irreversibly deleting a record and merely archiving it. If you merely archive a record or store it 'off-line' it must still be necessary to hold it and you must be prepared to give subject access to it and comply with the data protection principles. If it is appropriate to delete a record from your live system you should also delete it from any back-up of your information you keep.
5. The various organisations sharing information should have an agreement about what should happen once the need to share the information has passed. In some cases the best course of action might be to return the shared information to the organisation that supplied it without retaining a copy. In other cases, for example where the particular issue that the information sharing was intended to deal with has been resolved, all the organisations involved should delete their copies of the information. Paper records can cause particular problems. It can be easy to overlook the presence of old paper records in archives or filing systems. The various organisations involved in an information sharing initiative may need to set their own retention periods for information. However, if shared information should be deleted, for example because it is no longer relevant for the initiative's purposes, then all the organisations with copies of the information should delete it. If the information has a statutory retention period that has been exceeded, you must make sure that any organisation that has a copy of the information also deletes it. It might be possible to anonymise the information, in which case it can be retained indefinitely.
6. A good way to do this is to regularly audit the personal information you hold to make sure that information is not being retained for too long or deleted prematurely.

5. Security of shared information

The law

Personal information shall be protected by appropriate technical and organisational measures.

Your code of practice should do the following.

1. Describe ways of evaluating the level of security that needs to be in place.
2. Set out standards for the technical security arrangements that must be in place to protect shared information.
3. Describe the organisational security arrangements that must be in place to protect shared information.

Points to remember

1. Your key consideration should be to make sure that your security is adequate in relation to the damage to individuals that a security breach could cause. More sensitive or confidential information therefore needs a higher level of security. However, rather than having different security standards for different pieces of information, it might be easier to adopt a 'highest common denominator' approach, that is, to afford all the information you hold a high level of security. A good approach is for all the organisations involved in information sharing to adopt a common security standard, for example, ISO17799 or ISO27001. Adopting the Government Protective Marking Scheme can also help organisations to make sure there is consistency when handling personal information.
2. A difficulty that can arise when information is shared is that the various organisations involved can have different standards of security and security cultures. It can be very difficult to establish a common security standard where there are differences in organisations' IT systems and procedures. You should address problems of this sort before you share any personal information. It is the primary responsibility of the organisation providing the information to be shared to make sure that it will continue to be protected by adequate security once other organisations have access to it. There should be arrangements in place that set out who is allowed to access or alter a record.
3. Different organisations may have different cultures of security, and considerations similar to those outlined in the point above apply. Again, it is important that any relative weaknesses in an organisation's security are rectified. This could be done by the organisations involved delivering a common training package, before any personal information is shared between them. Where an organisation employs another organisation to process personal information on its behalf, a contract must be in place to make sure the information remains properly protected. In some cases, for example where very sensitive information is involved, staff may be subject to a vetting procedure. If vetting is justified, staff from other organisations that have access to the information should be subject to equivalent security procedures.

6. Access to personal information

The law

Individuals have a right of access to information about them.

Your code of practice should do the following.

1. Set out ways for making sure people can gain access to information about them easily.
2. Provide alternative ways for giving people access to their records.
3. Describe ways of making sure that a person gets access to all the information he or she is entitled to.
4. Give guidance on advising the public about the uses, sources and disclosures of information about them.
5. Provide guidance about relevant exemptions from the right of subject access, that is, cases where information will be withheld from a person who makes a request for access.

Points to remember

1. Where information is being shared between a number of organisations it can be difficult for people to work out how to gain access to all the information that's held about them. It is good practice to provide a single point of contact for people to go to when they want to access their information, and to make people aware of this facility.
2. Organisations are required by law to give people access to information about them in a permanent form. For most records, you can charge a fee of £10 and you must give access within 40 calendar days. However, it is good practice to provide faster, cheaper ways for people to gain access to information about them. This could be done by showing people their records when you come into contact with them or by setting up facilities to allow records to be viewed securely on-line.
3. When personal information is shared between several bodies it can be difficult to determine what information is held. It's very important, therefore, that organisations sharing information adopt good records management practices, to allow them to locate and provide all the information held about a person when they receive an access request.
4. When an organisation receives a request for personal information, it is required by law to also describe the purposes for which the information is held and its recipients, that is, who it is disclosed to. This part of the right of subject access is particularly important in the context of information sharing. You are also required to provide the individual with any information you have as to the information's source. In some cases information about someone may have been provided by another individual. This might be the case, for example, where a child's social work file contains information provided by a concerned neighbour. In cases like that, information about the source should normally be withheld.
5. Whether or not an exemption applies depends on the information in question, and in some cases on the effect that releasing the information would have on the individual. However, organisations dealing with a particular type of record are likely to find that they wish to rely on the same exemptions in respect of the access requests they receive. If this is the case, it would be useful to provide detailed advice to staff about how a particular exemption, or exemptions, work. It is good practice to be as open as possible with the public about the circumstances in which you will withhold information from them. In some cases this will not be possible, for example where telling a person that you hold exempt information about them would prejudice the purposes of law-enforcement by 'tipping off' an individual that he or she is being investigated.

7. Freedom of Information

The law

The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 give everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

Your code of practice should do the following.

1. Encourage the inclusion of material about information sharing in your FOI publication scheme.
2. Give advice on providing assistance to members of the public who make requests for a mixture of personal and non-personal information.

Points to remember

1. Most, if not all, public sector bodies involved in sharing information are covered by the Freedom of Information Act. This means they are required to include various information that they hold in their FOI publication scheme. It is good practice to include the 'paperwork' relating to information sharing in the publication scheme, including any relevant code of practice. There is a strong public interest in members of the public being able to find out easily why information is being shared, which organisations are involved and what standards and safeguards are in place. Making your 'paperwork' available to the public proactively should help to reassure individuals and to establish an increased level of trust and confidence in your organisation's information sharing practices.
2. Often people will make requests for information that cover both personal and nonpersonal information. For example, a person may request information about them that is being shared between various agencies and information about those agencies' policies for sharing information. Data protection and freedom of information may be dealt with by separate parts of your organisation, and a hybrid request may have to be dealt with under both pieces of legislation. However, it is good practice to be as helpful as possible when dealing with requests of this sort, especially as members of the public may not understand the difference between a data protection and an FOI request. (This framework code of practice does not contain recommendations about the handling of mainstream freedom of information requests. The Information Commissioner has published comprehensive advice about this elsewhere.)

8. Review

It is very important to regularly assess whether your sharing of information is having the desired effect, for example in terms of reducing crime or providing a more efficient service to the public. When assessing your information sharing it is also important to consider any complaints or questions that you have received from members of the public. You should keep your information sharing procedures under review, and should update your documents when necessary. Codes of practice and other documents can soon become out of date, given the rapid changes that can take place in an organisation's information sharing practices. When something goes wrong, for example, a security breach, it is important to find out the cause of this and to take action to prevent it happening again.

In particular, you should check whether:

1. Your sharing of information is having the desired effect.
2. Your fair processing notices still provide an accurate explanation of your information sharing activity.
3. Your procedures for ensuring the quality of information are being adhered to and are working in practice.
4. Organisations you are sharing information with are also meeting agreed quality standards.
5. Retention periods are being adhered to and continue to reflect business need.
6. Security remains adequate and, if not, whether any security breaches have been investigated and acted upon.
7. Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.

Appendix 1 -
The data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

   (a) at least one of the conditions in Schedule 2 is met; and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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

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

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

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

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

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

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

This is not a full explanation of the principles. For more information, see our Legal Guidance.

Appendix 2 -
Example of a simple information sharing procedure

Procedure for sharing information between Newtown Constabulary, Reporter to the children's panel and social work departments.

1 Contact details

1.1 Named individuals in Council Social Work departments and Area Children's Reporters.

2 Types of information

2.1 Child Protection Initial Report Form NM/59/2 to be sent to appropriate Social Work Department and Children's Reporter. These will be marked CONFIDENTIAL.

2.2 Memoranda as required. These will always be marked CONFIDENTIAL.

2.3 Crime reports may also be disclosed.

2.4 Verbal information will be shared at case conferences. This information will be either RESTRICTED or CONFIDENTIAL. Minutes should be classified according to the value of information in them.

3 How to handle the information

3.1 Transmission

3.1.1 RESTRICTED information can be transmitted over the telephone or sent by fax. CONFIDENTIAL information must be sent in a double envelope with the protective marking shown on the inner one.

3.2 Storage

3.2.1 All information must be kept under lock and key when not in the personal custody of an authorised person. The "need-to-know" principle will be strictly enforced. CONFIDENTIAL information needs to be protected by two barriers, for example, a locked container in a locked room.

3.3 Release to third parties

3.3.1 No information provided by partners to these procedures will be released to any third party without the permission of the owning partner.

Appendix 3 -

Other relevant guidance from the Information Commissioner available at www.ico.gov.uk

- Sharing personal information: Our approach. (A general position paper on information sharing.)
- Data sharing between different local authority departments.
- The use and disclosure of information about business people.
- The Crime and Disorder Act 1998: data protection implications for information sharing.
- Sharing information about you. (Advice to the public about information sharing.)

Appendix 4 -

Other sources of advice and guidance

- Audit Commission: www.audit-commission.gov.uk
- Cabinet Office: www.cabinetoffice.gov.uk
- Chief Information Officer Council: www.cio.gov.uk
- Communities and Local Government: www.communities.gov.uk
- Department for Children, Schools and Families: www.dfes.gov.uk
- Department of Health: www.dh.gov.uk
- Essex Trust Charter: www.essexinformationsharing.gov.uk
- Improvement Service: www.improvementservice.org.uk
- London Connects: www.londonconnects.gov.uk
- Ministry of Justice: www.justice.gov.uk
- National Archives: www.nationalarchives.gov.uk
- Public Record Office of Northern Ireland: www.proni.gov.uk
- Records Management Society: www.rms-gb.org.uk
- Society of Archivists: www.archives.org.uk
- The Scottish Government: www.scotland.gov.uk

Annex H - Information Commissioner's existing powers of investigation, inspection and enforcement

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, including the ability to:

- Assess compliance with the DPA or the data protection principles at the request of someone directly affected by the data processing (s42). In effect, this amounts to a complaints-handling function, but the formal outcome is limited to an 'assessment' without any compensatory or penal sanctions;

- Issue an Information Notice requiring a data controller to provide information requested by the Commissioner in whatever form he requires (s43). This information must be relevant to making an assessment under s42 or to determine whether a data controller is complying with the data protection principles. Failure to comply with an Information Notice, including knowingly or recklessly providing false information, is an offence;

- Make an assessment, with the consent of the data controller, of any processing of personal data for the following of good practice (s51(7)). This amounts to an audit power, but the requirement to seek consent renders it weak and of limited value;

- Inspect, operate and test equipment used for the processing of personal data - but only where the data are held in the Europol, Schengen and European Customs Information Systems (s54A);

- Enter and inspect premises - but only if a court will issue a search warrant, in cases where the Commissioner has reasonable grounds for suspecting a contravention of the data protection principles or the commission of an offence under the Act. It is an offence to obstruct the execution of a warrant or to fail, without reasonable excuse, to give any reasonable assistance when requested; and

- Issue an Enforcement Notice (s40) requiring a data controller to take, or refrain from, any specified action in order to ensure compliance with the data protection principles.

Annex I - International privacy law

Republic of Ireland’s Data Protection Act 1988

24. Powers of authorised officers.
24. (1) In this section "authorised officer" means a person authorised in writing by the Commissioner to exercise, for the purposes of this Act, the powers conferred by this section.
(2) An authorised officer may, for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions, on production of the officer's authorisation, if so required-

(a) at all reasonable times enter premises that he reasonably believes to be occupied by a data controller or a data processor, inspect the premises and any data therein (other than data consisting of information specified in section 12 (4) (b) of this Act) and inspect, examine, operate and test any data equipment therein,

(b) require any person on the premises, being a data controller, a data processor or an employee or either of them, to disclose to the officer any such data and produce to him any data material (other than data material consisting of information so specified) that is in that person's power or control and to give to him such information as he may reasonably require in regard to such data and material,

(c) either on the premises or elsewhere, inspect and copy or extract information from such data, or inspect and copy or take extracts from such material, and

(d) require any person mentioned in paragraph (b) of this subsection to give to the officer such information as he may reasonably require in regard to the procedures employed for complying with the provisions of this Act, the sources from which such data are obtained, the purposes for which they are kept, the persons to whom they are disclosed and the data equipment in the premises.

(3) Subject to subsection (5) of this section, subsection (2) of this section shall not apply in relation to a financial institution.
(4) Whenever the Commissioner considers it necessary or expedient for the performance by him of his functions that an authorised officer should exercise, in relation to a financial institution, the powers conferred by subsection (2) of this section, the Commissioner may apply to the High Court for an order under this section.
(5) Whenever, on an application to it under subsection (4) of this section, the High Court is satisfied that it is reasonable to do so and is satisfied that the exigencies of the common good so warrant, it may make an order authorising and authorised officer to exercise the powers conferred by subsection (2) of this section in relation to the financial institution concerned, subject to such condition (if any) as it thinks proper and specifies in the order.
(6) A person who obstructs or impedes an authorised office in the exercise of a power, or, without reasonable excuse, does not comply with a requirement, under this section or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect shall be guilty of an offence.

New Zealand's Information Privacy Principles

Principle 1 Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 2 Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

(a) That the information is publicly available information; or

(b) That the individual concerned authorises collection of the information from someone else; or

(c) That non-compliance would not prejudice the interests of the individual concerned; or

(d) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

Principle 2 subclause (2)(d)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word "tribunal" for the word "Tribunal".

(e) That compliance would prejudice the purposes of the collection; or

(f) That compliance is not reasonably practicable in the circumstances of the particular case; or

(g) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3 Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) The fact that the information is being collected; and

(b) The purpose for which the information is being collected; and

(c) The intended recipients of the information; and

(d) The name and address of—

(i) The agency that is collecting the information; and

(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law,—

(i) The particular law by or under which the collection of the information is so authorised or required; and

(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

(a) That non-compliance is authorised by the individual concerned; or

(b) That non-compliance would not prejudice the interests of the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

Principle 3 subclause (4)(c)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.

(d) That compliance would prejudice the purposes of the collection; or

(e) That compliance is not reasonably practicable in the circumstances of the particular case; or

(f) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4 Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) By unlawful means; or

(b) By means that, in the circumstances of the case,—

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5 Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 7 Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) To request correction of the information; and

(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8 Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9 Agency not to keep personal information for longer than necessary
An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.
Principle 10 Limits on use of personal information
An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) That the source of the information is a publicly available publication; or
(b) That the use of the information for that other purpose is authorised by the individual concerned; or
(c) That non-compliance is necessary—
(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) For the enforcement of a law imposing a pecuniary penalty; or
(iii) For the protection of the public revenue; or
(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

Principle 10 paragraph (c)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—
(i) Public health or public safety; or
(ii) The life or health of the individual concerned or another individual; or
(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or
(f) That the information—
(i) Is used in a form in which the individual concerned is not identified; or
(ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11 Limits on disclosure of personal information
An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

Principle 11 paragraph (e)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information—

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12 Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007 (to the extent to which those rules apply for the whole of that Act excluding the 1973, 1988, and 1990 version provisions).

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Section 6 principle 12(2): amended, on 1 April 2008, by section ZA 2(1) of the Income Tax Act 2007 (2007 No 97).

Subclause (2) was amended, as from 1 April 1995, by section YB 1 of the Income Tax Amendment Act 1994 (1994 No 164) by substituting the words “section OD 7 of the Income Tax Act 1994” for the words “section 8 of the Income Tax Act 1976”.

Subclause (2) was amended, as from 1 April 2005, by section YA 2 Income Tax Act 2004 (2004 No 35) by substituting the words “Income Tax Act 2004” for the words “Income Tax Act 1994”.

Data Sharing in Australia

The Australian *Privacy Act 1988* makes transparency a key requirement of information sharing. The Information Privacy Principles (IPP) contained in section 14 of the Privacy Act regulate information sharing between Government departments.

IPP 11 is about the disclosure of personal information. This permits information sharing where it is reasonably necessary for criminal law enforcement, or for the enforcement of all law imposing a fine, or for the general purpose of the protection of public revenue. This covers a broad range of purposes. It also provides that the disclosure of personal information is permissible where *"… the individual concerned is reasonably likely to have been aware… that information of that kind is usually passed to that person, body or agency"*.

Under IPP 1, information must be collected as necessary for a lawful purpose directly related to a function or activity of the collector. Under IPP 2, the collector shall take reasonable steps in all the circumstances, to ensure that the subject is aware of the purpose of collection and the circumstances where it will be disclosed. It should be noted that there is minimal judicial guidance on this principle as there has been no case law to date. It is also worth noting that the Australian Taxation Office and assistance agencies must comply with the *Data-matching Program (Assistance and Tax) Act 1990 (Cth)* and guidelines issued by the Privacy Commissioner under the Act to govern the conduct of data matching using tax file numbers.

The Privacy Commissioner has also issued advisory *Guidelines for the Use of Data Matching in Common Administration* for voluntary adoption by agencies conducting matching other than the programs specifically regulated by the 1990 Act. These Guidelines apply when a tax file number is not used in the matching process. However, that particular piece of primary legislation is quite outdated and the Australian Attorney-General is currently undertaking an inquiry into the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia. The inquiry, scheduled for completion in March 2008, is prompted by a number of considerations including the rapid advances in IT and changing community perceptions of privacy.

Data Sharing in Canada

In Canada, the law permits information sharing between public bodies but requires it to be transparent. Section 8 of the Canadian *Federal Privacy Act* regulates the disclosure of personal data by government institutions. Circumstances in which information sharing is permitted without consent include:

- for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
- for any purpose in accordance with any Act of Parliament or any regulation made there under that authorises its disclosure;
- for the purpose of administering or enforcing any law or carrying out a lawful investigation;
- to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

- for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or disclosure would clearly benefit the individual to whom the information relates.

This final point is particularly useful in that it provides a broad power for information sharing that is in the public interest and proportionate.

Produced July 2008