Privacy and data-sharing

The way forward for public services

A PERFORMANCE AND INNOVATION UNIT REPORT – APRIL 2002

Privacy and data-sharing

The way forward for public services

A PERFORMANCE AND INNOVATION UNIT REPORT – APRIL 2002

CONTENTS

More detailed annexes can be found on the PIU website:

www.piu.gov.uk/2002/privacy/report/index.htm

These annexes cover:

FOREWORD BY THE PRIME MINISTER

We all provide personal information to organisations providing services – whether supermarkets, banks, local authorities or the NHS. We do so because we know that it helps them to provide us with a better service. But we also expect organisations to use that data responsibly, to keep it secure and to respect our privacy.

New technologies, and the Internet in particular, mean that personal information is likely to become increasingly important both to the economy and to public services. In part that is because it is becoming cheaper and easier to collect, distribute and analyse information. In part it is because people expect services – whether public or private – to be better tailored to their needs, and better joined up.

But the public also wants to be sure that their privacy is protected.

All this raises significant challenges for public services. The public sector holds a huge amount of data. Some of that information – such as health records – is very personal and needs to be treated very sensitively. In other areas such as crime and fraud it is vital that the public sector makes better use of information to achieve results.

This is an important area for the Government to set the right strategy. If public services get it right, there will be important benefits for the transition to the knowledge economy. That is why I asked the Performance and Innovation Unit to look at the issues of privacy and data-sharing in delivering public services and to chart the way forward. The results of that study are published in this report.

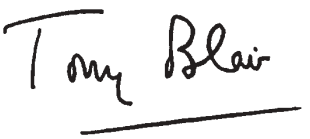
The report concludes that there is great potential to make better use of personal information to deliver benefits to individuals and to society, including through increased data-sharing. But these benefits will only be realised if people trust the way that public services handle their personal data.

The Government strongly supports the twin objectives set out in the report of encouraging better use of personal data to deliver improved public services and safeguarding personal privacy. We first set out our commitment to privacy in the 1999 Modernising Government White Paper. This report sets out the evolution of that commitment against a background of rapid developments in e-government and on-line services more generally.

There are a number of recommendations in the report where we need a proper debate before final decisions are made. On those recommendations – set out in the report – we are seeking views from all interested parties.

For the other recommendations, we want to see early progress in taking them forward as part of the strategy for delivering the overall objectives.

The opportunities are clear: better, more personalised, more efficient public services which handle personal information in a way that commands public trust.



Tony Blair
Prime Minister

1. EXECUTIVE SUMMARY

Key Points

Why are the issues of privacy and data-sharing important?

- The ability of the public sector to deliver high quality services, develop well-targeted policies and ensure efficient government depends on the effective use of knowledge and information – including personal information about citizens (such as health records, tax returns, welfare benefits, law enforcement records, driving licence information and so on). Handling this data raises a wide range of issues about privacy and the balance between individual rights and the common good.

- As we move to a society and economy based on information and knowledge, every business and public organisation will need to respond to the challenges involved in handling data. If the public sector can do so effectively, then there will be considerable benefits for the transition to a knowledge economy.

- Five main forces are pushing issues of privacy and data-sharing higher up the policy agenda, increasing their visibility and importance and requiring governments to develop a new approach:

  – citizens increasingly expect the public sector to provide more seamless and personalised services, to address the needs of particular groups in society and to tackle specific problems. This requires more joined-up approaches to the use of personal data across organisations;

  – changes in technology are beginning to transform the public sector with the move to electronic delivery of public services and the increasing ability of public services to make effective use of large amounts of electronic data;

  – public services have always had a responsibility to ensure that they are confident about the identity of the individual receiving the service, have the right data about individuals available, and can keep that data secure. More joined-up service delivery, together with more remote interactions through new technologies, raise new challenges in these areas;

  – the legal framework for human rights issues and privacy has been evolving rapidly, and will lead to significant changes in the relationship between the citizen and the state; and

- there are signs that public concern about privacy is on the rise – both in the private and public sectors – partly as a result of the drivers of change described above. This public anxiety has some parallels with the public's shifting attitudes to food safety over the last decade.

- Public services are already using data more effectively to deliver good quality services, understand problems, and design and deliver innovative solutions – but could do more.

- There is huge potential to make better use of personal data in public services to deliver benefits to individuals and to society, including through increased data-sharing. However, this will only be realised if the public trusts the way the public sector handles its personal information.

Rights and responsibilities for the public

- The public has both rights and responsibilities in the approach to the use of personal data in delivering public services. Citizens have formal rights and legitimate expectations that privacy will be protected while data are used to deliver tangible benefits.

- Citizens also have responsibilities, for example to provide accurate data, not commit fraud or other criminal activity, respect civil judgments and so forth. And the public rightly expects Government to play a role in ensuring that all members of society respect these responsibilities. This will often involve the use of personal data without the consent of the individual.

What objectives should the Government have?

- Government should pursue the twin objectives of enhancing privacy and making better use of personal data to deliver smarter public services. It is possible and desirable to achieve both.

- Achieving the twin objectives requires a more strategic approach by the public sector. This should be underpinned by four main principles:

  - using the data available in the most efficient and effective way possible to achieve goals;

  - adopting the least intrusive approach – i.e. where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so, recognising that the protection of privacy is itself a public service;

  - wherever possible, and where the benefits of better use of personal data are for the person using the service, giving citizens more choice in the management and use of their personal data to deliver public services; and

  - ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in

the policy-making process of striking a balance between individual rights and the wider public interest.

- In applying these principles to decisions about the need for increased data use or data-sharing, public services should systematically:
  - assess the benefits of the proposed data use/data-sharing in meeting public policy objectives;
  - consider alternative approaches to achieving the objectives which have a lesser impact on privacy;
  - identify the costs and risks of increased data use/data-sharing, recognising that many of the risks to privacy will be difficult to quantify;
  - assess safeguards that would minimise the risks (for example, using privacy enhancing technologies); and
  - use the accumulated evidence to strike a balance between the benefits and the costs and risks.
- Where increased data-sharing is proposed after this analysis, policy makers should therefore be in a position to explain why the public interest will benefit and that the proposed action is a proportionate response to the public policy objective.

What is the strategy for achieving the objectives?

- The strategy requires significant change in five broad areas:
  - building greater public trust in the way public services handle personal information;
  - putting in place new incentives and arrangements to improve the accuracy and reliability of personal data held by the public sector;
  - using new technologies to support more secure and more joined-up data use;
  - modernising the way the public sector manages information and privacy; and
  - achieving a clearer understanding of the operation of the legal framework and consulting on possible changes to improve legislative processes for establishing data-sharing gateways, in line with the twin objectives and principles set out in this report.

What are the areas for early action?

- In addition, public services should make early progress in a number of specific areas where personal information can be used more effectively in delivering services; where the public can be given greater assurances over the use of their own data; and where data can be used to improve efficiency.

The personal data held by the public sector are central to its ability to deliver high quality services…

1.01 This report aims to set out a new strategic approach to the use of personal data held by the public sector. The motivation for this new approach is twofold:

- first, an increasing recognition of the importance of effective and intelligent use of the personal data held by the public sector in delivering modern public services which better meet the needs of citizens; and
- second, an equal recognition that the public has both formal rights and legitimate expectations that personal privacy will be protected.

1.02 The public sector receives, uses and stores a huge amount of personal information about citizens. The focus of this report is the personal data used to deliver public services – such as health records, tax returns, welfare benefits, law enforcement information, local authority records, driving licence data and so on. The report looks at the use of this data within public sector organisations – including issues of data-sharing and data-matching across public sector boundaries.

There is huge potential to make better use of this data to deliver benefits to the public…

1.03 There are three main areas where there is considerable potential to make better use of personal information to deliver benefits to the public:

- better, more joined-up and more personalised public services – particularly in enabling e-government;
- more effective and better targeted policy making and evaluation; and
- more efficient public services, including using data to improve value for money and streamline services, to help tackle crime and fraud, and improve the effectiveness of the enforcement of civil judgments, criminal court fines and breaches of community penalties.

… and increasing expectations from the public for more joined-up and personalised public service delivery

1.04 Public expectations of public services are increasing, partly due to the way that the private sector is using technologies to deliver faster, more convenient, more joined-up and more personalised services. This is leading to greater demand on the public sector to use the information it holds more intelligently to do the same.

1.05 Technological change presents the public sector with new opportunities that make using and sharing data much easier and more affordable. It also presents opportunities to give citizens greater involvement in the use of their own information and in protecting their privacy. It is important to be aware of these developments and to take advantage of any that are relevant. But it is also important to recognise that technology is an enabler – not an end in itself: the focus must be on the changes needed to deliver benefits to citizens.

1.06 At the same time, the legal framework has been evolving rapidly – notably through the Human Rights Act 1998 (HRA), the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FoI) – and will lead to significant changes in the relationship between the citizen and the state.

This report is not a review of the legislative framework on privacy issues – rather it takes this changing legal position as one of the starting points in looking at the challenges and opportunities in making more intelligent use of personal data to deliver a step change in services and ensuring that privacy is indeed protected.

But this potential will only be realised if the public trusts the way the public sector handles their personal data – and protects their privacy

1.07 Public trust in the way that public sector organisations handle their personal data – and protect their privacy – is vital to the relationship between the citizen and public services. There are concerns that information technology – with more remote interactions and the greater use of personal information that it allows – could be a threat to privacy and lead to mistaken identity, inadvertent disclosure of private information and inappropriate transfer of data. There are some signs that the level of public concern about privacy is on the rise – for example, with an increasing proportion of people saying that they regard the right to personal privacy as very important. This anxiety has some parallels with shifting attitudes to food safety over the last decade.

1.08 The Government made clear in the Modernising Government White Paper that "data protection is an objective of information age government, not an obstacle to it".[1] This report strongly supports that statement, and looks at how to make it a reality. It is clear that if the public does not trust the way that the public sector handles personal information, then it will not be possible to achieve the potential benefits for individuals and for society from better use of data. In particular, this would put at risk the potential gains for the public from the move to the electronic delivery of public services.

1.09 More generally, as we move to a society and economy based on information and knowledge over the next decade, every business and public organisation will need to respond to the challenges involved in handling personal information. If the public sector can do so effectively then there will be considerable knock-on benefits for the transition to a knowledge economy and to the UK's position as a global e-commerce leader.

The vision must therefore involve twin objectives – enhancing privacy and making better use of personal data to deliver better, more trusted public services

1.10 This report recommends that public services should pursue the twin objectives of enhancing privacy and making better use of personal data to deliver smarter public services. These aims are *not* mutually exclusive. It is possible and desirable to achieve both.

1.11 While research suggests that people tend to identify risks from data use more readily than the benefits, it also shows that the public is able to identify a range of benefits from better use of data – such as faster service, greater convenience, increased simplicity and better accessibility. The challenge for the public sector is to tackle concerns about risks whilst delivering these benefits.

1.12 In many fields there does not have to be any 'trade-off' between individual privacy and the public good: the privacy and

[1] See www.cabinet-office.gov.uk/moderngov/whtpaper/index.htm – page 57 of the White Paper in particular.

accuracy of personal data can be improved alongside measures to share data between different agencies. However, in many cases judgements will have to be made. Much of the business of government already involves making difficult choices about how to balance the public interest and individual interests in relation to everything from taxation to policing, public health to transport. However, this report aims to set out some common elements which should be followed in pursuing the twin objectives of enhancing privacy and making better use of personal information, as a matter of good government.

1.13 As a first step in pursuing the twin objectives, this report identifies four high-level principles to guide public services' actions. These are:

- the public sector has a responsibility to use the data available to it in the most efficient and effective way possible to achieve its goals;
- in looking at information requirements, the public sector should adopt the least intrusive approach – i.e. where it can achieve improvements in services or efficiency without requiring more information and affecting personal privacy, it should do so, recognising that the protection of privacy is in itself a public service;
- wherever possible, and where the benefits of better use of personal data are for the person using the service, citizens should have a greater say in how their personal information is used to deliver public services; and
- ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in the policy-making process of striking a balance between individual rights and the wider public interest.

There are a number of issues to be addressed in achieving the vision

1.14 This project has identified five main barriers to realising the vision:

- there is a lack of public trust in the way that the public sector handles personal information and the security of that information, and some concern about the risks to personal privacy from technological change;
- the quality of personal information held by the public sector is variable, making better use of data and effective data-sharing much more difficult;
- the public sector is not making the most of new technologies which could help ensure that business processes meet citizens' needs and concerns;
- the current approach within public sector bodies to the collection, use and sharing of personal information is not consistent, and there are a range of administrative barriers to more effective data use; and
- there needs to be greater awareness of the legal framework, and clear and consistent safeguards covering data use.

1.15 Some action is already in hand to tackle these issues – for instance, progress is being made on the Government's 2005 target for 100 per cent on-line availability of government services, and moving beyond these targets. The UK online government portal – which provides a single entry point for all electronic government services – is already up and running. As an example of joining up services and making better use of data, UK online ran a change of address pilot

whereby people could choose to notify a number of departments, organisations and businesses at the same time, and only once, that they had changed address.[2]

1.16 But there is a need for a much more vigorous and strategic approach. This report sets out a strategy requiring significant change in the following five areas:

- building public trust;
- improving the accuracy and reliability of personal data held by the public sector;
- using new technologies to support more secure and more joined-up data use;
- modernising the way the public sector manages information and privacy; and
- achieving greater understanding of the operation of the legal framework and consulting on possible changes to improve legislative processes for establishing data-sharing gateways.

1.17 The following sections set out the key recommendations in each of these areas for realising the vision.

Building public trust

1.18 If the potential benefits of more effective use of personal data are to be realised, the public sector needs to build greater trust in the way that it handles personal information. This report recommends further action in the following areas:

- **clear and consistent principles should govern the way personal information is used right across the public sector.** This report publishes for consultation an overall Public Services Trust Charter setting out these principles. It makes clear the commitment to privacy as a fundamental human right, underpinned by legislation, and communicates the standards of service and care by which the public sector should be judged. It should be backed up for individual services by more specific Privacy Statements and Codes of Practice;
- **access to personal data should be improved, together with simple processes for correcting mistakes.** Public services should ensure that they are able to respond to requests from the public for access to their personal data quickly and efficiently, and should periodically report against this commitment. Organisations should have plain language explanations of access rights and subject access request procedures. Procedures to enable the public to correct their personal information should also be improved and simplified;
- **all public sector organisations should have a named senior manager with clear responsibility for the handling of personal information,** and a clear first point of contact on websites and in other publications for members of the public with concerns. This would build on the approach already adopted in many public sector bodies, for example the role of Caldicott guardians in the NHS; and
- **public sector bodies should ensure citizens are aware of their rights and what the law allows.** In all DPA and FoI-related publications, public sector bodies should use plain language and focus on their specific audience. The Information Commissioner should also take a more active role in promoting public awareness of data subjects' rights.

[2] The pilot was an experiment in the use of commercial services for public sector purposes, and worked by providing a link to such services.

Improving the accuracy and reliability of personal data held by the public sector

1.19 The achievement of the twin objectives of promoting privacy and better use of data depends crucially on the accuracy and reliability of the data available. Inaccurate data both increase the risks to privacy and decrease the ability of the public sector to deliver better targeted, more personalised services. Data quality can too often be seen as someone else's responsibility within organisations. This report recommends that it needs a higher profile and stronger management, and in particular recommends that:

- to improve the accuracy of data, and reduce the potential for mistakes or inappropriate use when data are shared, **public bodies should introduce basic standards for key items of data, and for labelling data sets** (in terms of their purpose, scope and limitations). This should lead to fewer mistakes and reduce one major cause of public concern;
- **standards for measuring data accuracy and reliability for privacy and data-sharing purposes should be developed** to enable public sector organisations to assess their performance, benchmark against others and set targets for continuous improvement. This should include issues of 'fitness for purpose'; and
- **internal and external audits should be used across the public sector to improve data accuracy and reliability.** Public service providers should consider whether consultation on new data-sharing proposals – particularly where information will be shared without the individual's consent – should include the outcome of data quality audits for the existing databases involved to ensure sufficient reliability. This will be a valuable diagnostic tool, ensuring that only good quality, up-to-date information is used in new initiatives.

More secure and more joined-up data use

1.20 Public services have always had a responsibility to ensure that they are confident about the identity of the individual accessing the service, have the right data about individuals available, and can keep that data secure. More joined-up service delivery, together with more remote interactions with public services through new technologies, raises new challenges in these areas. Public services need to respond in a way which delivers increasing security of identity and personal data, together with more joined-up services. In addressing these challenges, there are a number of emerging technological solutions to privacy issues and ways of using technologies to support data-sharing. The public sector needs to make better use of these emerging technologies as part of the wider strategy to improve public trust and deliver better services. This report recommends that:

- **the Government should give further consideration to strengthening the procedures for establishing the identity of those about whom it holds data, especially where the risks of fraud are greatest;**
- **the Government should encourage the development of an improved infrastructure for the protection of data and the authentication of transactions, for example through public sector pilots.** Further work will be needed to identify potential pilot areas and develop business cases. The pilots should test the

functionality and infrastructure necessary, and encourage interoperability with the private sector;

- **clear and visible safeguards should be put in place to prevent misuse of data and ensure that data are collected, stored and handled securely.** As part of the Government's e-government commitments, all central government departments should be in a position to reliably manage their electronic information as corporate records by 2004. This will provide them with an integrated infrastructure for secure and reliable management of accurate and up-to-date information. The public sector as a whole should at least match best practice in the private sector for information security, including adopting the ISO17799 standard and its associated processes.[3] The Government should actively monitor the development of new safeguards that could enhance the protection of personal data; and
- **to give citizens increased choice over the use of their own data and improve security, Government should develop a larger programme of smart card pilots in a range of services, ensuring that interoperability is a key feature of system design.** These pilots should also be developed in line with the principles set out in the e-Envoy's developing Smartcard Framework, including ensuring card-holders have access to the information that is held on the card.

Modernising the ways the public sector manages information and privacy

1.21 Improving the public sector's approach to issues of privacy and information management is essential if the potential benefits to individuals and society are to be realised. Other programmes, such as the move to electronic government, are already driving change. However, more action is needed. This report recommends that:

- **public sector bodies should identify a Chief Knowledge Officer at Board level.** The Chief Knowledge Officer should bring together a number of relevant functions (as determined by the needs of the organisation, including, for example, legal compliance and business redesign) to ensure effective integration of data management and privacy protection into mainstream decision making;
- **the public sector should adopt a more consistent approach to making decisions on data-sharing, together with increased transparency and consultation in the decision-making process.** This more consistent approach – to be achieved using the analytical framework set out in this report – should ensure that data-sharing and other proposals are assessed in terms of the size of the benefits of the proposed actions in relation to the costs and risks. For major changes in the use of data and data-sharing, public sector organisations should consider whether to publish and consult on a Privacy Impact Assessment;
- **overall responsibility for co-ordinating and driving forward the strategy set out in this report should be part of the responsibilities of the Lord Chancellor's Department (LCD).** Co-ordination of the strategy across the public sector will rest on LCD's ability to build links across all the key stakeholders, enabling the sharing of best practice and guidance on what works and monitoring the success of new initiatives;

[3] Central government is already committed to achieving ISO17799.

- **the cadre of information management professionals in the public sector should be supported and developed** – existing training and education programmes should be adapted to build expertise in the field of records and data management and privacy protection, focusing on the legal, technical and ethical issues. Action is needed to address the skills shortage so that public services can deliver against their commitments to get it right every time; and
- **incentives should be put in place to ensure that public services are able to work together to provide joined-up services and meet citizens' demands for new and reconfigured services** – in part by ensuring that Departments consider how initiatives to support better data use can be mainstreamed within their existing, and future, financial plans.

Clarifying and improving the legal framework to benefit citizens and improve trust

1.22 The current legal framework is complex and has a number of pieces of overlapping regulation. There is a need for greater clarity and, over time, a revised framework that reflects the twin objectives and principles set out above. As public services become increasingly joined up to focus on the needs of particular client groups (such as children) or to tackle particular problems (such as crime), there is also a need to ensure that the legal framework does not 'lock in' data use to particular organisational forms. The framework needs to be flexible enough to respond to new priorities and changes in public sector organisation and departmental structures. This report therefore recommends that:

- **guidance should be issued to all public sector organisations on the broad legal framework applicable to data-sharing and privacy issues.** This should be accompanied by clearer communication with the public, and increased training for public servants; and
- **the Government should consult on two proposals for legislative reform:**
  - **the introduction of a general power to enable public authorities to share personal data with the consent of the individual; and**
  - **changes to the legislative processes for establishing data-sharing gateways, to allow such gateways to be introduced through secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny.**

Specific opportunities for early action to deliver benefits to citizens through more intelligent use of personal data

1.23 The project has identified a number of specific areas where public services should make rapid progress in using personal information more effectively in delivering services; in using data more intelligently to improve efficiency; to tackle crime and fraud and to enable better enforcement of court judgments. These are set out in the box overleaf and in Chapter 11.

Specific opportunities for early action

Progress in several of these areas may be dependent on organisations securing statutory backing and resources in the usual way.

1. More joined-up and responsive services

Identifying and supporting children at risk of social exclusion: Local agencies need to be able to share information to identify children at risk of social exclusion quickly and provide the support they need to keep them on track. The Children's Fund has been established as a new part of the Government's strategy to tackle child poverty and social exclusion. The Fund will support services to identify children and young people between the ages of 5 and 13 who are showing early signs of difficulty, and provide them and their families with the support they need to overcome barriers and disadvantage and start achieving their potential.

Issuing photocard driving licences: The Driver and Vehicle Licensing Agency (DVLA) and the UK Passport Service (UKPS) have a long-standing agreement to exchange information to assist efficiency and customer service in the issuing of photocard driving licences. Data-sharing links with UKPS would allow applicants to supply their UK passport number to allow the details to be confirmed without the need for sight of the original document. It is hoped a pilot scheme will start running later this year.

Better access to health records: The NHS Plan requires radical modernisation in information management and technology (IM&T) infrastructures to deliver integrated services across all NHS organisations and with local authorities with social services responsibilities. The Information Policy Unit is developing a strategic outline case for broader national infrastructure services to develop closer working relationships with local authorities and other partners.

Services for those in real need: Legal aid eligibility is currently means-tested, and many eligible customers are benefit claimants. Better data-sharing between the Department for Work and Pensions (DWP) and the Lord Chancellor's Department (LCD) would eliminate duplication of effort and provide better security against fraud.

Ex-offenders: On leaving prison, many offenders do not have access to the services and support they require to help them resettle effectively into society. Better use of information by a range of services – including probation, welfare, social services, education, housing and others – would provide a more joined-up response to individual needs. The Social Exclusion Unit is conducting a survey into reoffending, and will be making recommendations for change in the way services are provided.

Modernising civil registration: The civil registration system in England and Wales will be modernised to enable on-line registration. This will continue to secure individuals' basic rights but be much more flexible. It will allow citizens to register births and deaths in a variety of ways including by telephone or the Internet.

Improving services for families (i): Sure Start aims to ensure that families with young children receive the services that are right for them by better understanding each family's social and medical situation. The legal permissions for data-sharing are restrictive or unclear. The result is that it is proving very difficult for partnerships to collate the necessary range of information. Some partnerships have dealt successfully with these difficulties by agreeing amongst the partners a data-sharing protocol that spells out key common practices and allocates responsibilities. The Sure Start Unit aims to share examples of good practice in guidance that will be available nationally.

Improving services for families (ii): Services for families are increasingly delivered locally, by a range of partnerships and service providers. Some families are unaware of the services that are available, or of the services they might be eligible for. Using the Child Benefit database would enable public services to send targeted information to parents, drawing their attention to the services offered in their region, and giving contact details for further information.

Streamlining services for motorists: The Driver, Vehicle and Operator (DVO) group in the Department for Transport, Local Government and the Regions (DTLR) is working to restructure its service delivery processes around customer needs. The DVO group holds much data about its customers and needs to improve its use of this data to provide more effective, joined-up services to the end user.

Improving information on the property market: The Land Registry, Valuation Office and Stamp Office are currently restricted in the amount of information they exchange and share. Changes could rationalise data collection, and provide aggregate data on the local environment, improving policy making and the information available to homeowners.

2. More effective and better targeted policy making

Helping children in need: Every year a substantial number of children are lost from the school rolls and become 'invisible' to local education authorities. Better data-sharing between local agencies would enable all services to be tailored to meet their specific needs, ensuring that they are able to make the most of their potential.

Better use of statistical and management information: Drug Action Teams (DATs) provide treatment services for drug addicts in the community. Better use of anonymised health data would enable DATs to evaluate the success of treatment programmes and initiatives, and would enable them to highlight where further resources would clear backlogs or target help at specific populations.

Getting the best from private providers of education and training: The Department for Education and Skills (DfES) has commissioned consultation on proposed new ways of working with providers of services to the public. New ways of working include an aim to improve the focus on outcomes by, amongst other things, modernising the approach to funding and contracting. One strand of the new proposals is to approve private providers on the basis of their past performance, not only in contractual matters, but in training and education outcomes.

Improving urban planning and investment: The Valuation Office Agency (VOA) collects floor space information to arrive at figures for the rateable value of such properties. There is considerable scope to use the VOA data more widely and at a more detailed level to allow local authorities to effectively monitor town centres, and provide planning inquiries with the information essential for making informed judgements on the impact of new development proposals. Improvements will translate into better planning of urban redevelopment, and into analysis of demand hotspots and local priorities.

3. Tackling crime and fraud

Better authentication: Both UKPS and the Criminal Records Bureau (CRB) need to confirm the identity of their applicants. Access to data held on public and private sector databases will permit corroboration of an individual's identity history in a more robust and cost-effective way than at present.

Tackling vehicle crime: Making more information available to the police at the roadside will enable better enforcement. Forces need to work towards implementation of data-sharing enabled in legislation, so that officers can have roadside access to all the information needed to enforce the law and make roads safer.

4. Tackling debt

Towards effective enforcement (i): About 60 per cent of enforcement in the county courts is ineffective because the claimant cannot find the necessary information about the debtor to enable them to take the right method of enforcement. LCD's review of enforcement proposes allowing a regulated enforcement agent, as an officer of the court, to have a limited ability to access information from designated third parties in order to confirm that the data provided by the creditor on the identity and whereabouts of the debtor are accurate so that the enforcement agent can make initial contact with the debtor.

Towards effective enforcement (ii): Currently, creditors have full control over the enforcement process and it is up to them to gather any necessary information and decide which method of enforcement will be carried out by the court. LCD's review of enforcement proposes introducing a mechanism for creditors to obtain a Data Disclosure Order in circumstances where debtors have proved wilfully non-compliant with previous court orders. A Data Disclosure Order would enable the courts to initiate a process to apply for information from designated third parties about the address of the defaulter/debtor's employer, whether the defaulter is in receipt of benefits and the address to which those benefits were being sent, and the extent of the debtor's financial assets in bank or building society accounts.

Enforcement of civil obligations in Scotland: The Scottish Executive is currently reviewing the law of enforcement of civil obligations in Scotland and will consult on proposals for reform. Part of this review is about the obligation for the payment of money and covers the problems experienced, by public and private creditors, in the enforcement of debts owed to them. It is clear that creditors' access to a range of information about debtors' financial circumstances and assets would enable appropriate and effective enforcement mechanisms to be targeted to avoid procedures which are likely to be fruitless or excessive.

Implementation

1.24 The strategy set out in this report will require early action in key areas, with longer-term work to assess the implications for large-scale pilots involving new technologies. Early work should focus on areas where benefits for citizens can be quickly realised, including:

- wherever possible, making progress on the specific proposals set out in the box above;
- development of service-specific **Privacy Statements**, Codes of Practice and model protocols;
- plain language **explanations of citizens' rights** and information-sharing activities; and
- identifying clear **contact points** for all data issues.

1.25 Public services should also identify internal actions to ensure that the strategy set out in this report can be delivered effectively. Work should include:

- decisions on the implementation of **Chief Knowledge Officer** roles;
- steps to improve **data quality**;
- reflecting the report's conclusions in overall **business design**; and
- using the **analytical framework** in assessing new data-sharing initiatives.

1.26 Work in the following areas, by contrast, will need to take place over a longer time scale:

- consultation on **possible legislative changes** to allow data-sharing with the consent of the individual and to improve legislative processes for establishing data-sharing gateways; and
- development of proposals to pilot **smart card and public key cryptography** in the public sector.

1.27 This report sets out three recommendations for consultation:

- the Public Services Trust Charter (recommendation 1);
- legislative reform to allow public authorities to share data with the consent of the individual (recommendation 24); and
- legislative reform to the legal processes for establishing data-sharing gateways (recommendation 25).

1.28 The Government would welcome views on these proposals. Responses should be sent in by 12 July 2002 to:

Paul Henery
Freedom of Information & Data Protection Division
Lord Chancellor's Department
Room 912
50 Queen Anne's Gate
LONDON SW1H 9AT

Fax: 020 7273 2684

E-mail: foiu@homeoffice.gsi.gov.uk

1.29 The Lord Chancellor's Department will take lead responsibility for implementation, working closely with the Cabinet Office and other departments. Resources for this implementation work will be considered as part of the current Spending Review. The implementation plan set out in the report is dependent on appropriate resources being available. A revised implementation plan will need to be developed at the end of the consultation process, taking account of the responses to consultation on specific proposals and the available resources.

1.30 The Lord Chancellor should report on progress with implementation of the strategy set out in this report 12 months after publication. Departments should also report on progress as part of their annual reporting cycle.

2. INTRODUCTION

Background

2.01 The development of a society and economy founded on information and knowledge is already transforming the ways in which personal data are collected, stored and used. Over the next decade the approach to data, information and knowledge is set to become a critical issue for every business and public body.

2.02 Some of these issues are already having a visible impact on many sectors – from banks and retailers to on-line services. But it is in public services that the challenges are set to be particularly acute, both because society has a huge amount to gain from more effective use of information by the public sector, and because the risks from the possible abuse of personal information are far greater due to the volume, coverage and nature of the data involved.

2.03 In the light of this challenge, the Performance and Innovation Unit was asked to develop a strategy that would enable government to deliver 21st century public services while setting in place the safeguards and mechanisms that would inspire confidence in the public sector's handling of personal data. If the public sector can respond effectively to the challenge, there will be considerable knock-on benefits for the transition to a knowledge economy.

Coverage of the report

2.04 The issues of data use are examined within the context of public sector organisations and across public sector boundaries, including central and local government. As the devolved administrations are responsible for many aspects of service delivery, consideration of the conclusions contained in this report would fall within their jurisdiction.

2.05 The report does not consider 'G2B' – government to business – relationships in detail, but has shared the research undertaken by the Comprehensive Business Directory study project.[4] In many aspects of service delivery, businesses will have a corporate identity that is treated as 'personal information'. As such, this information should be managed in the same way as citizens' information, and the strategy set out in this report would apply.

Services provided by contractors or in PPPs

2.06 A number of services are outsourced or managed through Public Private Partnerships (PPPs) – for example, on IT systems. The principles and objectives and the strategy set out in this report apply equally to information held on systems wholly owned and operated by public sector organisations as well as those that are outsourced or involve private or voluntary sector partners. A general principle of this

[4] See www.business-info.gov.uk

report is that any organisation responsible for delivering public services should be subject to these principles and objectives.

Personal data use

2.07 This report refers to better data use as a means to deliver public services and to enable better-targeted policy making. The term data use is a catch-all term for use of personal data within and between departments, agencies and public bodies, including the sharing of data for purposes other than those for which it was originally collected. This can include:

- case-by-case sharing of information in support of service delivery – data are usually identifiable, as service providers need to ensure that the customer is who they say they are and is receiving the full service they are entitled to. Information exchange is dependent on gateways and takes place under controlled circumstances, with set safeguards and security measures. The informed consent of the individual is often a requirement in information exchange;
- bulk exchange of data for policy making and statistical research – in these instances, information is anonymised or pseudonymised to ensure that the information cannot be traced back to an identifiable individual. As such, data-sharing is less dependent on gateways and administrative triggers, but is still subject to safeguards and security measures to ensure data remain anonymous and to prevent misuse. Individual consent is not needed, as information is anonymised;
- bulk exchange of data, for example for crime prevention – information usually relates to specific, identifiable individuals and is shared through set statutory gateways in controlled circumstances, with agreed safeguards to prevent misuse of data. Information exchange does not rely on the consent of the individual; or
- case-by-case sharing of data for investigation of crime or fraud in specific cases – information will normally be identifiable, as the identity of the criminal or fraudster (and occasionally their associates) needs to be known. Information disclosure is dependent on set administrative triggers, such as the opening of a criminal investigation or prosecution, and is often regulated through an authorising officer. Data exchange is not dependent on the consent of the individual.

Structure of this report

2.08 The report sets out a strategy for better delivery of essential public services through better use of personal data, and describes the safeguards that will need to be put in place. Accordingly, the chapters that follow are:

- Chapter 3: Drivers of change
- Chapter 4: Current practice
- Chapter 5: Objectives and principles – A strategy for the future
- Chapter 6: Building public trust and engagement
- Chapter 7: Improving data accuracy and reliability
- Chapter 8: More secure, more joined-up data use
- Chapter 9: Managing information and privacy
- Chapter 10: The legal framework
- Chapter 11: Service specific proposals
- Chapter 12: Implementation

Financial implications

2.09 This report contains 25 recommendations and 19 service specific proposals, all of which will require action by public sector organisations. There will be additional net costs to government in the short to medium term, although these should be manageable within Departmental Expenditure Limits (DELs).

2.10 Immediate costs will arise for the Lord Chancellor's Department in co-ordinating the strategy. However, personnel requirements should not be large – at least at first – and staff could be found through a reorganisation and refocusing of current functions. Similarly, some immediate costs could fall on individual organisations in setting up Chief Knowledge Officer functions. This report explicitly envisages gradual integration of functions and responsibilities, so costs should be subsumed within existing baselines. Where public bodies are net exporters of data to others and consequently incur additional costs in carrying out the recommendations within this report, we would expect partner agencies which benefit from the supply of data to contribute to the costs.

2.11 One set of recommendations in the report that will need exceptional financing will be the possible piloting of smart cards and public key cryptography. Resource implications will need to be considered in the normal way following initial work to assess the case for pilots, including outline proposals and detailed cost-benefit analyses.

3. DRIVERS OF CHANGE

Summary

Five main forces are pushing issues of privacy and data-sharing higher up the policy agenda, increasing their visibility and importance and requiring governments to develop new approaches:

- public expectations for more joined-up service delivery, 'smarter' public services and more effective solutions to problems – this is partly influenced by developments in the way the private sector is using technologies to deliver faster, more convenient and more integrated and personalised services;
- changes in technology are beginning to transform the public sector with the move to electronic delivery of public services – new technologies allow information to be used and shared much more easily;
- identification and authentication have long been important considerations for public services, but are being brought into sharper relief by the move towards e-government. The growth in identity fraud and identity theft is also increasing the risks for citizens and is leading to growing demand for more secure systems;
- the legal framework for human rights issues and privacy has been evolving rapidly, and will lead to significant changes in the relationship between the citizen and the state; and
- there are early signs that the level of public concern about privacy is on the rise, partly as a result of the drivers of change and partly because of a growing desire for greater personal control. This public anxiety has some parallels with the public's shifting attitudes to food safety over the last decade.

3.01 The ability of the public sector to deliver high quality services, develop well-targeted policies and ensure efficient government depends on the effective use of knowledge and information – including personal data about citizens. The use of personal data in this way raises a wide range of issues about privacy and the balance between individual rights and the common good.

3.02 The Government is strongly committed to protecting personal privacy – it has already:

- made clear in the Modernising Government White Paper that data protection is an objective of information age government, not an obstacle to it; and
- put in place a new legal framework with the Human Rights Act, Data Protection Act and Freedom of Information Act.

At the same time, Government is firmly committed to achieving rapid improvements in the quality, targeting and effectiveness of public services.

3.03 Against this backdrop, five main forces are pushing issues of privacy and data-sharing higher up the policy agenda:

- increasing public expectations for high quality, reconfigured services;
- the increasing penetration and potential uses of information technology;
- issues around identification and authentication;
- the evolving legal framework; and
- changing public attitudes to privacy issues.

3.04 The public sector's response to these forces should recognise that concerns for security and privacy of information can be addressed positively. This chapter looks at each of these driving forces in turn.

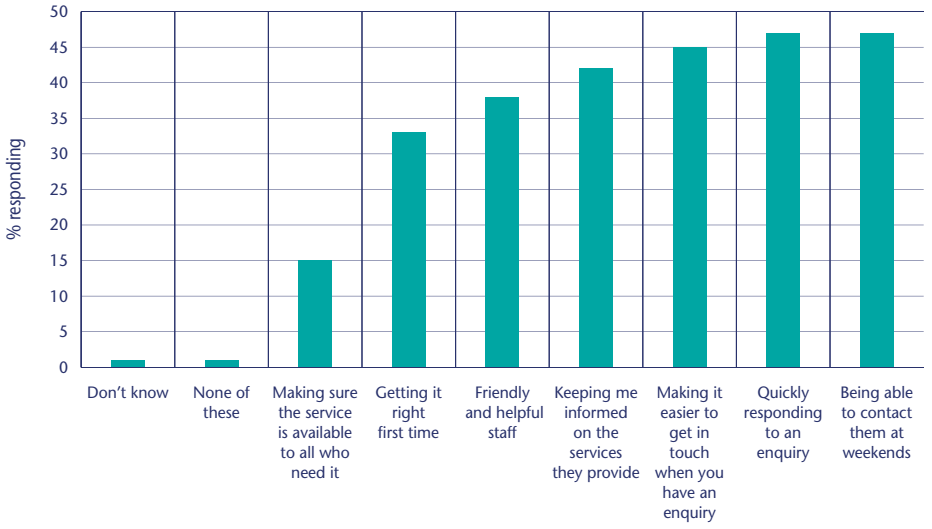
Increasing public expectations for better services

3.05 The public is demanding ever better quality, better-targeted public services and greater ability on the part of government to solve problems. Experiences of innovative private sector services and products are increasing already high expectations of public services.

3.06 Research shows that people are increasingly expecting immediate responses from public services and demand for innovative, responsive and high quality services is high and expected to grow. Over 40 per cent of people would like to send change of address details over the net and one third would like to fill in census or tax forms on-line. A survey by consultants Cap Gemini Ernst & Young also estimated that by 2003 a quarter of all banking transactions would be web-based. At present, however, actual use of the Internet for such transactions is low.

3.07 As Information Technology (IT) penetration rises, more and more people are taking advantage of the convenience of Internet services offered by the private sector and are applying their experience to their expectations of public services. Demand is increasing not only for better services but also for reconfigured services that allow for greater accessibility and flexibility, with more evidence of joined-up government in action.

Fig 3.1: Priorities for improvements to public services: "Which two or three of these, in your opinion, are aspects of public services that are most in need of improvement?"[5]



3.08 The First Wave of People's Panel surveys in 1998 noted that 40 per cent of respondents felt that public services did not meet their expectations; a further 20 per cent felt that services were 'infuriating' and only 23 per cent felt that public services were 'efficient'. Subsequent reports have highlighted clear areas for improvement, including reducing the time taken queuing or waiting, minimising referrals between officials, and simplification of procedures and documentation. Indeed, further research with the People's Panel has highlighted that the public demand for more accessible, quicker and more reliable services is high and likely to increase.

3.09 This demand for service improvements has also been reflected in research into e-government. A Cabinet Office study[6] found that people were able to identify core benefits from better use of their information:

- 76 per cent expected a faster service;
- 46 per cent expected greater convenience;
- 29 per cent were attracted by increased simplicity; and
- a further 25 per cent felt that better use of data would offer increased accessibility to public services.

3.10 Research into public attitudes towards the Change of Address function accessible through UK online echoed this demand.[7] Survey responses indicated rising expectations – people expected the system to be faster, and so simple to use that it would be free from user error, and to provide up-to-the-minute records of frequent users of public services. The challenge for public services is therefore to achieve a step change in service delivery – one way to achieve this is through smarter information management.

[5] Results from the People's Panel, Issue No. 5 (Cabinet Office, March 2000).
[6] *Electronic Government: the view from the queue* (Cabinet Office, October 1998).
[7] *Assessing Attitudes to the Change of Address Function: Government Portal Research* (Cabinet Office, January 2000).

Technology is transforming the business of government

3.11 Advances in technology present both challenges and opportunities in many different areas of government activity: the public is using technology as a way of simplifying their lives, and expects government to do the same; the Government is committed to both e-government and using technology to improve services and efficiency more broadly; and technology itself presents tools to both share data faster and better, and to protect privacy. It is important to be aware of these developments and to take advantage of any that are relevant, but it is also important not to be swept up by technology as an end in itself.

3.12 New technologies are providing new opportunities with major implications for public services and service users. For instance, more powerful IT platforms, with greater flexibility and the ability to communicate with other systems, allow for greater centralisation of service delivery – bringing together different databases with related information to form a single database with a more holistic view of a service and its consumers. But at the same time, technology also provides opportunities for more locally based solutions to specific community problems – using geographical information systems to map data on to postcodes and streets to provide an in-depth analysis of problems, enabling community-based solutions.

3.13 Technology is also enabling better use of personal information in different ways. In the past, information was held on discrete databases that were effectively isolated from other sources of information, and had a finite capacity for storing information. Advances in technology now mean that databases can hold much more information and it is much easier to link information between databases and to transfer data from one database to another.

Box 3.1: How technology enables data-sharing

Data-matching happens either 'off-line' or 'on-line'. Off-line, data from one database are downloaded and run against a different database. This practice allows information to be updated and for comparisons of data to highlight anomalies for further investigation, perhaps as incidents of fraud or to clarify or fill in missing information. In on-line data transfer, middleware systems allow the linking of different databases to create a single 'virtual' database, where data can be accessed, compared and updated from a single point. This system is often used in banking or insurance telephone call centres, to enable operators to deal with all but the most complicated queries quickly and efficiently.

In the public sector, the vast majority of data transfer is in bulk via magnetic tape or other media. The majority of the anomalies subsequently highlighted are simple keying errors that can be easily corrected. Other anomalies may be instances of fraud. But technology cannot identify this alone without human involvement – all data anomalies are referred to staff for further analysis and action.

3.14 The ability of new technology to manipulate information has implications for personal privacy. But privacy-enhancing technologies are also advancing and evolving rapidly, while processes and safeguards can be built into system design from the outset to ensure that personal privacy is protected. These safeguards can restrict access to information to selected public service workers, restrict the information that each official can access and can keep a rolling register of who has accessed what information and for what purpose.

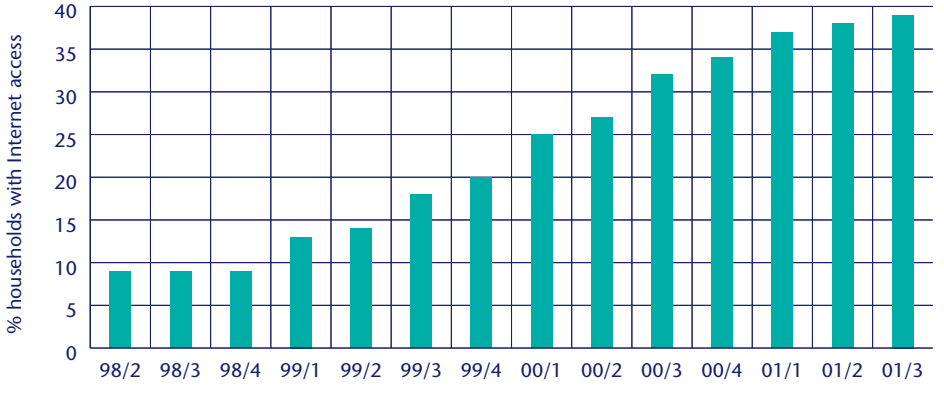
3.15 Technology can also improve consumer access to their personal information. UK online already gives individuals a standard method of accessing information held on all government websites. The Government Gateway[8] allows on-line transactions through use of authentication methods such as public key cryptography[9] to ensure that those requesting information are who they claim to be. From the privacy of their own homes, consumers will be able to access services and information as never before.

Technology is simplifying people's lives

3.16 Around 9.7 million households – 39 per cent of all UK households – already have access to the Internet from home, and this figure is set to grow further. More and more people are making increasing use of technology, and the Internet is fast becoming a feature of our daily lives.

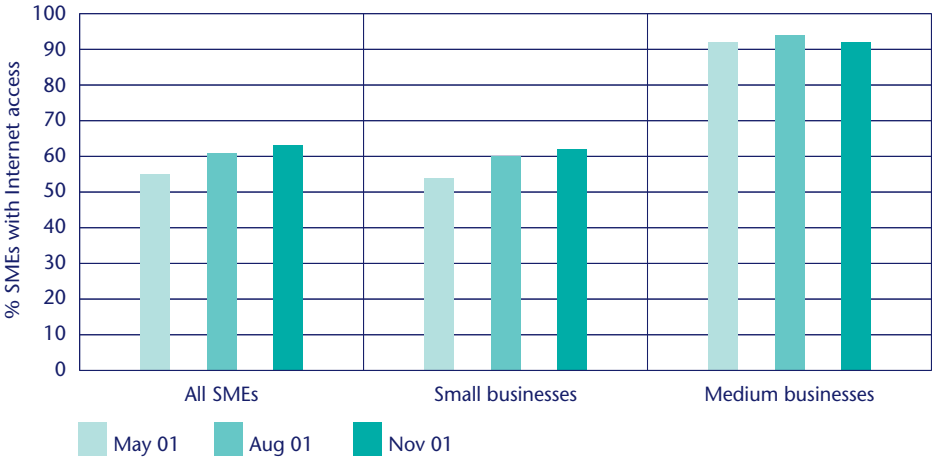
3.17 The growth in domestic Internet access and use is mirrored in the growth of UK e-commerce – the UK e-commerce market is now the biggest in Europe. Ernst & Young's Enterpriser Survey 2000, carried out by MORI, revealed an 80 per cent increase in e-commerce activity. At the beginning of 1999, just under 40 per cent of businesses were engaged in e-commerce; by the end of the year, almost 70 per cent of entrepreneurs were pursuing such opportunities.[10]

Fig 3.2: Households with home access to the Internet, UK: % by quarter[11]



[8] See www.gateway.gov.uk
[9] See Chapter 8.
[10] *UK Online: Annual Report* (Office of the e-Envoy, September 2000).
[11] *Internet Access* (ONS, 18 December 2001). This figure includes all forms of access, including new technologies such as digital television. A recent Oftel publication, *Effective Competition Review: Dial-Up Internet Access* (Oftel, 29 January 2002) estimated home access to the Internet was as high as 45% of UK households.

Fig 3.3: UK small and medium sized enterprises (SMEs) with Internet access – per cent[12]



3.18 Consumers are increasingly taking advantage of tailored products and services provided by new technology. Internet users, in particular, are significantly more likely to share private demographic information in return for personalisation. Consequently, the number of personalised websites has increased tenfold over the past two years.[13]

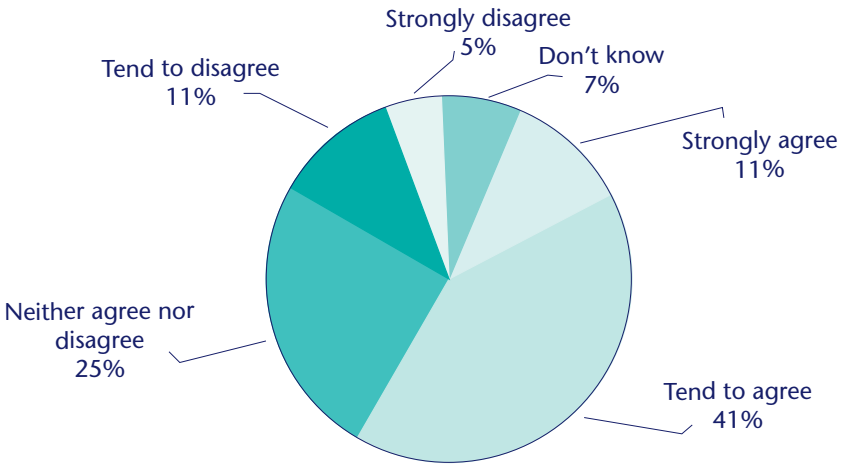
Improving government through technology

3.19 The pace of technological change will allow public services to provide more accessible, faster and more accurate services. Technology is providing public services with a major opportunity to personalise essential services and to allow consumers to choose for themselves how they interact with service providers – for instance through the Internet, a telephone call centre or face to face. The move to e-government, coupled with increasing use of technology and electronic processing of data, is enabling organisations to provide more customer-focused services.

3.20 In the UK, where expectations of public services have always been high, people expect public services to provide similarly integrated and individualised services. The First Wave Research with the People's Panel highlighted the fact that over half of the people surveyed believed that technology would facilitate their interactions with government:

[12] *Business use of Internet: Oftel small and medium business survey wave 7 November 2001* (Oftel, February 2002).
[13] *Privacy v Personalisation* (Cyber Dialogue, 2000).

Fig 3.4: "Do you agree or disagree that new technology will make it easier for you to deal with government?"



3.21 Increasingly, public sector organisations are working in partnership, using technology to manage information to deliver efficient, high quality services. Such collaboration relies on ready access to the relevant information to identify client groups and to target assistance where it is most needed. In addition to providing better services, technological developments allow public bodies to make better use of the non-personal information they hold – for example, geographical information systems can overlay data from a variety of sources to create maps of crime hotspots[14] enabling police forces to better understand local crime issues, and so tailor their responses accordingly.

3.22 As the basis for policy making, better data use and statistics can also improve the decisions Government takes to help key populations like children and senior citizens, as well as devising a holistic approach to helping socially excluded communities. Work is already in hand to tackle the gaps identified in the Social Exclusion Unit's PAT 18 report[15] which highlighted:

> *"the enormous use that government and communities could make of comprehensive and up-to-date information about social and economic trends in local areas. Better information would highlight problems when there was still time to nip them in the bud [and] would enable better diagnosis and solutions of complex joined up issues…"*

3.23 Overall, IT is a large part of the background to the Government's modernisation programme, including the move towards the electronic delivery of services. A key target in this area is that 100 per cent of government services should be available on-line and that everyone should have access to the Internet by 2005.[16] In

[14] See *Data Exchange and Crime Mapping: A Guide for Crime and Disorder Partnerships* (Home Office, May 2001) for an example. Also available at www.crimereduction.gov.uk/technology01.htm

[15] Social Exclusion Unit's *National Strategy for Neighbourhood Renewal – Report of Policy Action Team 18: Better information*, April 2000, The Stationery Office.

[16] See www.e-envoy.gov.uk/publications/reports/esd The e-Envoy's Summer 2001 report noted that of 520 services identified, 256 (51 per cent) are already available on-line, 386 will be available by 2002 (74 per cent), and at least 513 (99 per cent) by 2005.

meeting these targets, public services will need to focus on the benefits that can be derived for consumers – faster, more accessible services that meet users' needs rather than the convenience of service providers.

Identification and authentication are becoming more important with the move towards e-government and the rising incidence of identity fraud

3.24 Identification, authentication and entitlement are key issues for public service providers:

- identification – to establish who is accessing the service;
- authentication – to guarantee that the individual is who they claim to be; and
- entitlement – to ensure that the individual receives all the services they are entitled to.

3.25 With the growth of e-government, traditional forms of identification and authentication are less secure – identity documents, such as a passport – cannot be verified on-line and the service provider cannot actually see the individual accessing the service. With the move towards more joined-up services, enabling service users to use different channels to access services, identification issues and the ability to cross-check data and access all the relevant data in order to provide a seamless service gain further importance. Existing identification methods, which for public services rely on reference numbers such as the National Insurance number and NHS number, may not be sufficient by themselves to enable accurate linking of data or different data sets.

3.26 In order to provide joined-up, secure and seamless services for citizens, public sector organisations need to develop more robust mechanisms for verifying identity. A number of different approaches have been tested or adopted to tackle this problem. Some approaches rely on 'common identifiers' to enable simple linking of data. In other cases, systems are linked together to form a single 'virtual' database. But end-to-end action is needed to ensure that systems are robust – it would be insufficient, for example, to tackle identification when accessing a service without ensuring that traditional means of establishing identity, such as a passport or birth certificate, are secure.

3.27 There has recently been a growth in the prevalence of cases of identity theft and identity fraud in both the private and public sectors. There is also a growing link between identity fraud and organised crime, meaning that documents used to verify or prove identity can be forged easily and efficiently. This enables criminals to hijack or 'steal' someone's identity for fraudulent purposes. An example is obtaining a credit card in someone else's name with the intention of not paying the bill – it is estimated that there were more than 500,000 cases of identity theft in the USA in 1997 alone.[17] The incidence of identity theft in the USA led to the enactment of the Identity Theft Act in 1998, which made identity theft a criminal offence.

3.28 Identity theft is linked to organised crime in several ways, including:

- illegal immigrants require ID to access goods and services in this country;

[17] See US Government Accounting Office Report *Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited,* May 1998, GAO/GCD – 98 – 100BR, cited in *Identity Theft: Authentication as a Solution*, National Fraud Centre, March 2000, available from www.nationalfraud.com

- criminals engaged in money-laundering will rarely do so under their own identity – identity theft and fabrication constitute one of a number of ways of avoiding detection; and
- organised criminals can and do perpetrate large-scale frauds against the state and against private sector bodies through the use of false ID.

3.29 It is difficult to calculate the cost of identity fraud to the UK economy, but the available evidence suggests that it is at least £1.2 billion each year – although this is almost certainly an underestimate. A report for the Home Office and the Serious Fraud Office estimated that the total annual economic cost of all types of fraud could be as high as £13.8 billion.[18] In the public sector, fraud means that valuable resources are not spent where they are most needed.

3.30 The move to Internet and telephone transactions for business and public services means that existing systems for identification and authentication are no longer sufficiently robust. New systems will be needed to ensure that, for the individual, their identity is protected and their information is secure from external threats. For public services, better identification and authentication processes will lead to more efficient and more secure services, ensuring value for money and reducing the amount of waste and error.

The evolving legal framework is changing the relationship between citizen and government[19]

3.31 In the last three years key pieces of legislation have created broad rights to ensure that the privacy of people's personal information is respected:

- the **Human Rights Act 1998** incorporates the European Convention on Human Rights (ECHR) Article 8 right to respect for private and family life and enables people to enforce their rights directly in the UK courts;
- the **Data Protection Act 1998** regulates the manner in which personal data may lawfully be collected, handled and disclosed and provides a number of rights through which individuals can ensure that their personal data are used in a proper manner; and
- the **Freedom of Information Act 2000** will provide for public access to information held by public authorities. This includes an extension of individual rights to information held on them by public authorities regardless of how or where it is held.

3.32 In addition to the statutory regulation of data processing afforded by this legislation, the common law duty of confidentiality and public bodies' administrative powers – known as *vires* – also have a bearing on the extent to which public authorities can collect, use and share personal data.

[18] *The Economic Cost of Fraud,* a report for the Home Office and the Serious Fraud Office by National Economic Research Associates (March 2000).
[19] See also Annex A for a fuller discussion of the legal framework – www.piu.gov.uk/2002/privacy/report/index.htm

Box 3.2: Defining 'privacy'

The Human Rights Act 1998 incorporated the European Convention on Human Rights into UK law, including the Article 8 right to respect for private life. However, domestic law does not provide a single definition of the term 'privacy' and therefore what may be included in a 'right to privacy'. Definitions of 'privacy' are most often attempted by reference to its opposite – distinguishing that which is rightfully 'private' from that which is 'public'. Matters falling within the private sphere are distinguished from those in the public one; such matters may include a person's family, religion, health, sexuality and financial affairs. However, even these matters may yet be subject to legitimate public intervention – for example, in tackling crime – and so any definition of a 'right to privacy' inevitably produces qualifications. While it is possible to identify certain matters that may generally be 'private' or included in a 'right to privacy', any definition is inevitably subjective since it will depend upon an analysis of all the relevant facts and circumstances of the case.

Human Rights Act 1998 (HRA)[20]

3.33 The HRA guarantees fundamental human rights, including the right to respect for private and family life – privacy. The Act enables people to bring cases to enforce their rights directly in UK courts[21] and requires public authorities to act in a manner compatible with the rights it enshrines. The right to respect for private and family life is broad in scope and includes the collection, use and exchange of personal data.

3.34 The Article 8 Convention right is not an absolute right to privacy – it explicitly recognises that there is a balance between society and the individual, and that interference with people's privacy by public bodies is legitimate in certain circumstances. Public authorities may lawfully act in a way that interferes with the Convention right to respect for private life, but in doing so must show:

- a clear legal basis for their intervention;
- the aim of the interference must be the pursuit of one of the following legitimate aims:
  - national security;
  - public safety;
  - protection of the economy;
  - prevention of crime or disorder;
  - the protection of health or morals; or
  - the protection of the rights and freedoms of others; and
- the intervention must be necessary in a democratic society in the pursuit of one of the legitimate aims. In essence, public authorities must prove that there was no other way in which the aim could reasonably have been achieved that would have meant a lesser intrusion on people's rights.

[20] A copy of this Act and the others mentioned in this chapter is available on the HMSO website: www.legislation.hmso.gov.uk/acts.htm
[21] Individuals will still be able to take cases to the European Court of Human Rights, provided that they have exhausted all domestic remedies first.

Box 3.3: Defining 'Personal Data' (see also Data Protection Act – Sections 1 and 2)

Personal Data "means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of or is likely to come into the possession of, the data controller…" This includes publicly available information, such as the electoral register.

Sensitive Personal Data is defined in Section 2 of the DPA as data consisting of information on a data subject relating to their: ethnic or racial origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of offences and criminal convictions or proceedings.

The personal data held by public sector organisations normally covers key issues such as name and address and additional information as appropriate.

Data Protection Act 1998 (DPA)[22]

3.35 Citizens also have rights in relation to how information about them is collected, stored and used. The DPA regulates the processing of personal data – this includes the collection, holding, use, disclosure and destruction of personal data. Any handling of personal data must be in accordance with the provisions of the Act. In essence, compliance with the data protection principles entails the following, each of which has implications for data sharing:[23]

- the collection, use and disclosure of personal data must be fair and lawful;
- there must be transparency in the collection of personal data;
- personal data must not be processed in any manner incompatible with the purposes for which they were originally collected;
- personal data must conform to certain minimum standards of relevance and accuracy, and must only be retained where this is actually necessary;
- there must be levels of security proportionate to the sensitivity of the data and the risks to individuals; and
- data must be processed in accordance with the specific rights granted to individuals (data subjects) by the Act.

3.36 The Act provides exemptions to the subject information provisions, including national security (DPA s.28), crime and taxation (s.29) and health, education and social work (s.30).[24] In addition, Schedule 7 to the Act lists a further group of exemptions, ranging from matters such as the armed forces to legal professional privilege.

[22] The Act gives force to an EC Directive on Data Protection (95/46/EC) and derives ultimately from ECHR and the 1981 Council of Europe Convention on Data Protection. The Act does not apply to all personal data, but only to such information that is either processed automatically (i.e. on computer) or recorded manually (i.e. on paper) "as part of a relevant filing system" or which forms part of an "accessible record". See also definition of "data" in Section 1(1) DPA.

[23] The Act also regulates data transfer across national borders, preventing the transfer of data outside the European Economic Area unless there is an adequate level of protection for individuals.

[24] Other exemptions include regulatory activity (s.31), journalism, literature and art (s.32) and research, history and statistics (s.33).

3.37 Compliance with the Act is enforced by an independent public official, the Information Commissioner, who is also responsible for the enforcement of the Freedom of Information Act in England, Wales and Northern Ireland.[25] Data subjects have rights, which they can exercise directly and which may be independently enforced by the courts. The key rights include:

- the right of subject access – essentially the right to be told whether data controllers are processing their personal data, and if so to be given a description of the data, to be told the purposes for which they are being processed, information on sources and disclosures and potentially to be provided with a copy of the data;
- the right to have incorrect or inaccurate data corrected; and
- an absolute right to prevent the use of personal data for direct marketing purposes and a more qualified right to object to processing which causes unwarranted damage or distress.

Box 3.4: The role of the Information Commissioner[26]

The Information Commissioner, formerly the Data Protection Commissioner, is an independent public official responsible for implementation of the Data Protection Act 1998 and – except in Scotland where there is to be separate legislation – the Freedom of Information Act 2000. She reports directly to Parliament.

The first duty of the Commissioner is the promotion of 'good practice', defined as including but also extending beyond the enforceable requirements of both pieces of legislation. Both Acts envisage promulgation of advice to data controllers and public authorities and the development of Codes of Practice, and give the Commissioner the power to conduct good practice audits with the consent of the bodies involved. The Commissioner is also charged with promoting awareness of the legislation to citizens.

In addition to these general duties, the Commissioner has specific duties including the maintenance of the register of data protection notifications and the approval of publication schemes under the Freedom of Information Act, and has at her disposal a range of enforcement powers in the event of non-compliance with the minimum standards required by the legislation.

3.38 The courts have the power not only to order the deletion or rectification of inaccurate or misleading data but also to award compensation for any damage and associated distress that a breach of the Act has caused.

The Freedom of Information Act 2000 (FoI)[27]

3.39 FoI gives a right to access any information held by a public authority, and extends the right of subject access to certain personal information held by public authorities that is not covered by the DPA –

[25] In Scotland, a Scottish Information Commissioner will enforce the regime that will be implemented by the Freedom of Information (Scotland) Bill, laid before the Scottish Parliament in September 2001.
[26] See also www.dataprotection.gov.uk
[27] The Freedom of Information Act 2000 is not yet fully in force.

though there are a number of exemptions. In addition to the requirement to respond to individual requests for information, two features of FoI are of particular relevance to privacy and the use of personal data:

- the Act places an obligation on public authorities to develop publication schemes under which they routinely publish information as to how they do business, their objective, the basis of decisions and so forth. This requirement reinforces the requirement of the DPA for transparency; and
- it requires compliance with a Code of Practice on Records Management to be published by the Lord Chancellor. This reinforces the requirements of the DPA regarding data quality.

Ensuring a lawful basis for data-sharing

3.40 The DPA requires that personal data be processed lawfully. It does not generally specify what is or is not lawful processing. This can only be established by reference to the general law. There are four principal considerations:

- establishing a legitimate basis for processing: the first data protection principle specifies that all processing of personal data must satisfy at least one of a set of conditions set out in Schedule 2 to the DPA, and in the case of sensitive data (such as health data or data relating to criminal convictions) an additional condition set out in Schedule 3;
- necessary powers: public authorities must also ensure that they have the necessary powers – known as *vires* – to process personal data for a particular purpose. In order to disclose personal data to or to receive data from another public body they must have the necessary legal powers to do so;
- public authorities must also ensure that there are no specific statutory prohibitions on the processing or disclosure of personal data for any particular purpose;
- finally, a public authority must ensure that there are no more general legal rules or doctrines which prevent disclosure. In many cases while there may be no specific statutory prohibition on disclosure, the common law duty of confidentiality may make a disclosure unlawful.

3.41 These considerations frequently overlap and the important point to note is that they are cumulative.

Confidentiality

3.42 Obligations of confidence have evolved and been developed by the common law, but are also found in statute, and in contractual terms – as may happen when someone receives confidential information under an agreement that does not have contractual force, or when the recipient knows or ought to know that information has been imparted to them in confidence. Most kinds of information can form the subject matter of confidential communications. Crucially, it must be of limited public availability and must be clearly defined. Obligations of confidence can also arise by virtue of the existence of a relationship between the parties – for instance lawyer and client, but also familial relationships and those between friends.

3.43 There are limits to the extent of the duty of confidentiality. The duty of confidentiality will not protect illegality, gross immorality, or conduct contrary to public policy. Courts have found 'public interest' reasons for denying protection of confidence

when, for instance, disclosures of sharp industrial practices have occurred. There are also some statutory limitations on obligations of confidence, for example those contained in the Companies Act 1985 regarding the publication of balance sheets, profit and loss accounts, and auditors' reports. The Civil Procedure Rules contain probably the widest type of requirement to disclose, for the purposes of litigation, information that may be confidential and personal.

3.44 There are also time limits on the duration of the obligation. If the obligation arises out of an agreement between parties, this will depend on the terms of that agreement. Contracts of employment will therefore generally be subject to a requirement of reasonableness in the length of time for which an employee can be bound to keep a confidence. Similarly, restraints of trade may continue to bind ex-employees, but the longer the term and the broader the scope of matters which must be kept confidential, the more onus will be placed on the employer to show that the term is reasonable.

Confidentiality in the context of public services

3.45 When a member of the public provides their personal details to a public body, they expect that these details will be treated as confidential and will not be passed to persons other than the recipient – unless disclosure is necessary in the circumstances, or the data subject has been told that disclosures may be made. Whether a duty of confidentiality should be maintained has to be weighed against the powers and duties which a public body has to disclose the information. Obligations of confidence can, of course, attach to data that is not personal data within the meaning of the DPA.

Powers of public bodies to share data

3.46 When considering what powers one has to share data, one must first consider the type of public body one is dealing with. Generally speaking, a government department derives its powers from a number of different sources:

- specific statutory powers – known as information gateways – to share data with others;
- implied powers – the power to do anything that is necessarily incidental to express powers; and
- the 'Ram' doctrine[28] – i.e. a department can do anything that a natural person can, provided it is not forbidden from doing so.

3.47 By contrast, statutory bodies derive their power to act from their creating statute, and have no *vires* to act outwith their statutory functions. Local authorities are creatures of statute, and must act in accordance with statutory powers. However, they do also have a statutory 'implied' power (under s.111 of the Local Government Act 1972) to do anything ancillary to the discharge of any of their functions. Nevertheless, the powers of local authorities and statutory bodies are clearly not of the same broad scope as powers of government departments.

Data pooling – data-sharing within organisations

3.48 Where information is 'personal data', the second data protection principle provides that 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.

[28] This derives from advice by Sir Granville Ram, First Parliamentary Counsel 1937–1947.

3.49 One must always bear in mind the first data protection principle's requirement that the processing be 'fair'. Even though a secondary purpose may not be 'incompatible' within the literal meaning of that word, it may nonetheless constitute 'unfair' processing if it goes beyond that for which the data subject could reasonably expect their personal data to be used. Where the additional processing is quite different from the original reason for the acquisition of the data, it may be easier to allege unfairness.

3.50 The first principle's requirement that the processing must be 'lawful' should also be borne in mind. Among other things, this means that there must be an underlying lawful basis upon which to conduct the processing, whether that is derived from statute, common law, implied powers, or by any other means. A number of Acts of Parliament have been established to create data-pooling powers for public bodies, to enable them to share data within the organisation for the full range of purposes for which the body is responsible.

Information gateways – sharing data between data controllers

3.51 In a similar fashion to data-pooling powers, information gateways enable data-sharing between two organisations where the administrative powers are not thought sufficient to permit the proposed data-sharing. Information gateways are created in statute and generally specify the uses for which information obtained under their aegis must be used. Examples of statutory gateways include:

- **S.127, Finance Act 1972** which enables data-sharing between HM Customs and Excise and the Inland Revenue, "for the purpose of assisting them in the performance of their duties";
- **Ss.14 and 15, Teaching and Higher Education Act 1998** which allows the Department for Education and Skills to supply certain information about teachers to the General Teaching Councils for England and Wales; and
- **Ss.20 and 21, Immigration and Asylum Act 1999** which permits the supply of information to the Secretary of State for "immigration purposes", and by him to certain recipients for police, customs and other specified purposes.

3.52 Taken together, the legislative regulation of data processing, the limits imposed by administrative powers and the duty of confidentiality provide a good deal of protection for citizens in the collection, use and sharing of personal data. There have been considerable benefits to citizens achieved using personal data – including more joined-up service delivery and better policy making – through very specific legislative initiatives. However, the patchwork of legislation has also left citizens unclear about their rights and the degree of control over their own information, and public bodies unclear about how they can use personal data to improve services.

Public concern about privacy is on the rise

3.53 Partly driven by the changes described above, there are strong indications that public concerns about privacy and data use are becoming more marked, and raise important issues about the relationship between the citizen and the state.

3.54 Privacy and data protection are not areas that provoke strong *spontaneous*

feelings. Issues of more direct impact on daily life – such as health care, education and crime – are most readily quoted as being of highest concern. However, research suggests that when people are prompted – i.e. when given a list of issues, including privacy, and asked to identify the more important – privacy scores highly. Indeed, the Information Commissioner has found that, when prompted, only crime prevention and improving standards of education are thought to be more important issues for the public.[29]

3.55 The apparent latency of this concern about privacy is important because it suggests that it remains obscure to and unanticipated by public policy makers – if ignored and left unaddressed, it could arise quickly and unexpectedly. In the field of privacy and public sector use of information, this could carry the risk of seriously undermining society's trust in public services and lead to significant and long-lasting harm to the effective delivery of services, including implementation of integrated e-government services.

3.56 One example of disengagement brought on by distrust is the 1991 Census, where the 'missing million' people were significantly concentrated amongst young men, many of whom may not have engaged due to unfounded fears that their personal information would be used for Community Charge – Poll Tax – purposes. The box below is a recent lesson from the Canadian Government on the importance of securing public trust through an open and transparent process.

Box 3.5: The Longitudinal Labour Force File in Canada

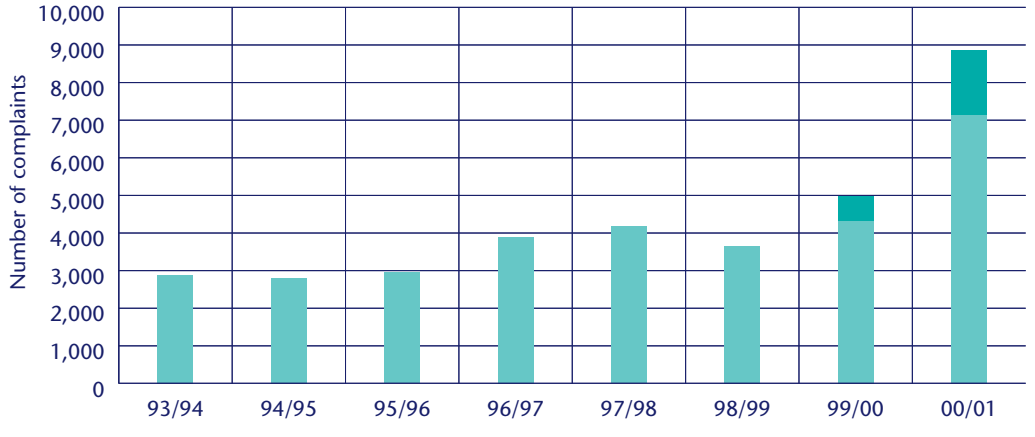
Human Resource Development Canada (HRDC), an agency created out of a number of federal departments and agencies, developed the Longitudinal Labour Force File.[30] The database was compiled largely without the knowledge of Canadian citizens, and with no public consultation. The Federal Privacy Commissioner[31] discovered that extensive longitudinal records containing up to 2,000 items of data on each individual were being compiled by bringing together data gathered by HRDC predecessor departments as well as information gathered subsequently by its various agencies and operational arms. The records included tax returns, benefit information, immigration files, welfare files from provincial and municipal levels, training information and employment and social insurance master files. The Commissioner's report resulted in a public outcry, the upshot of which was an announcement (on 29 May 2000) that the longitudinal file was being completely dismantled.

[29] *Data Protection Tracking Research 2001* (RSGB & Taylor Nelson Sofres, July 2000). Published with the Information Commissioner's Annual Report 2001.
[30] See labour-travail.hrdc-drhc.gc.ca/doc/lab-trav/eng (URL does not begin www).
[31] See www.privcom.gc.ca

3.57 There is evidence that privacy concerns are once more on the rise. More people than ever before are stating, when asked, that they consider the right to personal privacy very important. The latest research conducted by the Information Commissioner's Office found that 96 per cent of respondents saw protecting people's information as very or quite important and 73 per cent of adults were very or quite concerned about the amount of information that is kept by organisations.[32] There are other, less direct indicators of rising privacy concerns in the actions people are taking. For instance, a gradually rising proportion of people are taking up general privacy protection measures, such as ex-directory telephone numbers.[33]

3.58 Concerns about web privacy are a combination of fears about Internet security for financial transactions and of disquiet at the practice of Internet companies of surreptitiously tracking users or selling personal information databases. These are not directly transferable to privacy in relation to the public sector, but they do contribute to growing awareness of privacy issues more generally. Some of the growing awareness of privacy issues can be seen in the gradual increase in the number of cases referred to the Information Commissioner for assessment.

Fig 3.5: Complaints/requests for assessment received by the Information Commissioner 1990 to 2001[34]



3.59 Increasing concerns about privacy are in part due to a growing appreciation of the power of technology, and how developments in IT are enabling organisations to use data in new and innovative ways. For instance, there is an increasing awareness of the development of personal data-combining services on the Internet and the ease with which personal data held on a private database can be combined with publicly available data sets, such as the electoral register. This is a particularly powerful

[32] Data Protection Tracking Research 2000, for Information Commissioner by RSGB & Taylor Nelson Sofres, July 2000.
[33] Estimated 37 per cent of BT landline telephones were ex-directory in UK in 1997; 45 per cent in 2000. Recent research suggests that 90 per cent of future mobile phone users will opt to go ex-directory (private communication with BT).
[34] Taken from the Information Commissioner's Annual Report, June 2001. Figures for 1999/2000 and 2000/01 also include complaints regarding Telecommunications Regulations (the dark green section of the bar).

marketing tool in the private sector and has led to an increase in micro-marketing, which enables companies to use postcode-specific data to analyse social trends and patterns to enable specific targeting of services and products at a truly micro level.

3.60 To add to this complexity of generalised and non-specific privacy concerns, is the evidence of relatively low public awareness of what is actually done with their personal information[35] – different groups tend to under or overestimate the extent of data-sharing of personal information about them by public bodies. This lack of awareness of how personal information is used is sometimes linked to an individual's sense of having little control over it.

3.61 Public attitude research on privacy and data use, including some commissioned for this study, shows consistent themes around risks of data use, including:[36]

- unauthorised access to personal information;
- unauthorised informal disclosure of personal information;
- errors in data-handling;
- infection with inaccurate data;
- misidentification;
- unjust inference (essentially making decisions unfairly based on inferences from matched data); and
- use of 'soft' data (such as professionals' opinions or assessments of individuals as clients).

3.62 Acknowledging these risks, there are clear challenges for service providers in engaging with their stakeholders to constructively address public concerns about how personal data are used in delivering public services.

[35] 'Attitudes towards confidentiality and survey research: some results from qualitative research', ONS unpublished paper, Nov. 2000.
[36] *Strategies for Reassurance: Lessons from Focus-Group Research on Allaying Public Concerns about Privacy and Data-Sharing in Government* Perri 6, Strathclyde University (Cabinet Office, March 2002).

4. CURRENT PRACTICE

Summary

Public services are already increasingly using data effectively to deliver good quality services, understand problems, and design and deliver innovative solutions.

There are three main areas where progress has been made in making better use of personal information to deliver benefits to the public:

- **better, more joined-up and more personalised public services;**
- **more effective and better targeted policy-making; and**
- **more efficient public services, including using data to improve value for money and streamline services, to help tackle crime and fraud, and to enable better enforcement of court judgments.**

However, there is room to achieve much more.

4.01 The public sector is already beginning to use data more effectively to deliver services, understand problems, and design and deliver innovative solutions. This chapter sets out some existing initiatives – but it is clear that public bodies could do much more to deliver better, high quality services and pioneering solutions to problems through better data use and more data-sharing.

More customer-focused public services, better service delivery

4.02 Better data use can streamline a citizen's dealings with public services, by enabling a single point of contact to deal with all but the most complicated queries – a similar process already happens in banking, insurance and other telephone call centres. By enabling the service provider to access a range of relevant information, enquiries can be responded to more quickly and efficiently, and services can be tailored to meet the needs of the individual client. Better use of

information held in the public sector can therefore deliver a range of personal benefits, such as accessibility, responsiveness, and speed and accuracy of service.

4.03 Moves towards comprehensive electronic delivery of public services are already having an impact. NHS Direct is an innovative scheme that provides health care information and services through call centres and on-line. It will be developed further to include patient access to electronic personal records and electronic prescribing of medicines by 2004.

4.04 Box 4.1 below describes the approach taken in one health authority to providing a joined-up service for patients and carers while addressing the legitimate privacy concerns raised by better data use.

Box 4.1: West Surrey Electronic Health and Social Care Record Project

The West Surrey Electronic Health and Social Care Record Project is a new initiative involving collaborative working across primary and secondary health care and social services within Adult Mental Health Services and Older People's Services. Combining information from GPs, an NHS Trust (providing community and mental health services) and Social Services, an integrated electronic view of relevant records about an individual will be made available to Accident and Emergency, NHS Direct, the ambulance service, Social Services Emergency Duty Team and other Out of Hours services. The drivers for this project included:

- nationally, a lack of communication is regularly cited whenever a breakdown occurs in delivering a complex mix of community services to vulnerable people;
- complaints from service users and their carers that they are asked for the same information many times; and
- the need for integrated information to support joint health and social care teams.

It is expected that the project will deliver a range of benefits, including:

- Benefits for **service users** and **carers**
  - Better information about personal care
  - Faster service, fewer assessments
  - Less frustration, fewer errors
  - Enhanced confidentiality management
- Benefits for **staff**
  - Increased efficiency, fewer delays
  - Better decision making
  - Enhanced care planning processes

The basic philosophy behind the initiative is that integrated, seamless service delivery is impossible without integrated data. At the same time, the project has also recognised that

the benefits will not be fully realised without addressing issues of privacy and confidentiality. Three key principles underpin the project's approach to data-sharing:

- access on a **need-to-know basis**;
- subject to having obtained **informed consent** from the service user; and
- the organisations are **custodians** of information owned by the service user.

A working draft of a protocol covering the secure and confidential sharing of person identifiable information has been developed as part of the project, and will be signed by the Chief Executives and Caldicott Guardians of all the involved organisations. Partner organisations will also be responsible for developing a local policy and procedure to ensure they meet the requirements of the protocol.

4.05 The Department for Work and Pensions (DWP) has also established an on-line application service for a retirement pension forecast. The forecast tells you in current values the amount of pension you have already earned and the amount of state pension you can expect at state pension age based on what you have earned already and what you might earn before you retire.

4.06 At the local level, local authorities are exploring the use of one-stop shops for providing customers with the range of local government services at a single physical outlet or on a single telephone number. The success of these service centres rests on the sharing and combining of personal information held by different services within the council – instead of getting passed from agency to agency or person to person, a customer could have several enquiries dealt with at the same time. If successful, this can provide easy access and faster service for customers, and potentially reduce administrative costs.

4.07 Local authorities are often at the forefront of innovative service delivery, through the use of Customer Relationship Management techniques in delivering one-stop shops, using new IT solutions to existing problems and in reaching out to their communities. For example:

- the London Borough of Sutton is aiming to increase access to public service information by installing a series of 'I-Plus' public information kiosks;
- the London Borough of Newham has established six one-stop shops, backed up by a call/contact centre, providing better access to information and services and creating substantial administrative savings;
- Liverpool City Council is developing a network of 11 one-stop shops throughout the city, enabling the delivery of multiple services from the same location;
- Warwick District Council has launched the 'Open Door' project to provide citizens with a range of means with which to communicate with the council, fostering social inclusion; and
- Bristol City Council has launched an e-mail newsletter, 'e.Bristol', which will provide free monthly updates on the council's work.

4.08 Box 4.2 provides two further examples of how services are being reconfigured to provide better, more seamless services for citizens.

Box 4.2: Improving services

Better access

Hertfordshire County Council is setting up a £3.2 million gateway for the public to access the council and its services. The gateway will be made up of three elements: a telephone call centre (Herts Line); one-stop shops providing face-to-face advice as well as access to Internet equipment (Herts Enters); and the development of the Council's website so that services can be accessed on-line (Herts Online).

Faster service

The *Land Registry* is involved in a National Land Information Service (NLIS) project to provide a one-stop shop for land and property information. The service enables a customer to order searches on-line and view the results immediately. Results of searches and enquiries, which would normally take weeks, are available to the user within seconds. The Land Registry holds data on more than 16 million titles in England and Wales.

4.09 Better use of information can also ensure that services are targeted where they are most needed. For example, the Connexions and Sure Start initiatives bring together a range of local service providers to deliver services designed for the child's specific needs. The Connexions Service provides information, advice and guidance for all young people aged 13 to 19 to help them make the most of their educational and vocational choices and development opportunities during their teenage years. Sure Start aims to improve the health and well-being of children during their pre-school years, so they are ready to flourish when they go to school. Data-sharing enables the local agencies to better understand the problems, focus on the needs of specific client groups and deliver a holistic response to common problems, addressing the problem of disjointed service provision for young people and preventing children from falling through the gaps in service provision.

4.10 The 'Who Cares?' Trust, in partnership with the Department of Health and the Department for Education and Skills is developing a holistic set of interactive on-line services, for children in public care, called 'CareZone'. Children in care have the same potential to succeed as all other children but are significantly more likely to fail in education, suffer mental illness, experience unemployment and to fall into crime because they lack the appropriate support and help in getting information, making decisions and accessing services. The aim of CareZone is to give children more control over their lives by helping them to help themselves. CareZone combines a simple point of access to education, health and social services with a 'walled garden' where access by others is by permission only. It will also provide a 'virtual vault' of secure but permanently accessible personal information. Security and privacy features are rigorous in order to protect CareZone users from abuse – for instance from paedophiles – and to ensure privacy of the individual child's personal information.

4.11 Data-sharing can also help identify the extent and causes for non-take up of benefits and enable the effective targeting of

information to eligible non-claimants. For instance, Housing Benefit has a take-up of around 94–98 per cent while Family Credit has a take-up of only 73–79 per cent[37] – the fact that the Inland Revenue is running an advertising campaign costing £12 million to encourage take-up of the Working Families Tax Credit illustrates the scale of cost of generalised information campaigns that might be saved through more personalised targeting.

More effective and better targeted policy making

4.12 Government is already beginning to realise the benefits of better use of information in solving problems and identifying priorities for action – developing better, more effective policies requires knowing what works and what doesn't. Increasingly, policies are directed at social issues, and therefore increasingly involve personal data. By contrast, for statistical and research purposes, personal data can be completely 'anonymised' – information that can never be linked to individuals can be shared much more readily than identifiable personal data.[38]

4.13 Protection of more vulnerable populations, such as school age children, is another area where protecting privacy by anonymising information is important. For example, historically the planning of education provision by schools has been significantly hampered by the lack of reliable longitudinal data on the performance of individual pupils and of the effectiveness of the different schools attended over the course of a school career. But collection of longitudinal data on individual children presented the Department for Education and Skills (DfES) with a difficult issue – how to protect a child's privacy interests while also collecting the data necessary to improve the educational system? Box 4.4 below describes DfES's innovative solution to promoting both privacy and better data collection and use.

Box 4.3: Anonymous and pseudonymous data

There are examples where anonymous data is sufficient most of the time, but it may occasionally be necessary to trace certain kinds of information back to its origin. In this case, 'pseudonymous' storage may be preferable. Ideally, it should be the data subjects themselves who provide the link between the pseudonym and a real identity, but where this is not appropriate it is important to ensure that the number of other people who can do so is very limited. For example, the Medicines Control Agency has a 'yellow card' scheme for reporting adverse drug reactions.[39] Traditionally, doctors were asked to include patient names when filing reports. But now they use a local reference number, which has no meaning except within that surgery or hospital – the agency assigns its own number to each report, which it tells the doctor. This number is added to the patient's file and is used in future communications with the agency. Thus a series of data about an incident can be built up without the agency ever knowing the patient's name or identity.

[37] *Income Related Benefits: Estimates of Take-Up in 1998/99* (DSS, December 2000).
[38] The DPA also allows personal data to be used for secondary research purposes in certain circumstances.
[39] See www.open.gov.uk/mca/ourwork/monitorsafequalmed/yellowcard/yellowcardscheme.htm

Box 4.4: The Unique Pupil Number (UPN)

The Unique Pupil Number (UPN) is allocated to all pupils, facilitating the linking of records by DfES statisticians. The UPN deploys privacy enhancing technologies to ensure that the child's data are not misused and are used for research purposes only. Local reference numbers are allocated by schools, which are reported, together with records of academic achievement and other core information, to the Department. At this stage the local number is translated into a different, national number which is used for the purposes of the creation of the longitudinal record. While the system is somewhat complicated, the result is that the accuracy of record keeping has been improved by the use of a unique reference number, while the risk of unauthorised access to pupil records has been avoided through creative application of new technology. The net benefit is also that government will be able to better evaluate the success of different initiatives and different schools.

4.14 Another area where data can significantly improve policy making is the prevention of crime. Recent evidence[40] from the Home Office shows that half of all serious crime in England and Wales is committed by a mere 100,000 persistent offenders, 95 per cent of whom are men and half of whom are under 21. Nearly two thirds are hard drug users while around a third were in care as children. Half have no qualifications at all and three quarters have no work. They commit an average of 120 crimes each per year and, because they tend to be involved most in violent crimes, they are responsible for the majority of the estimated £60 billion per year cost of crime. Knowledge of these factors in generating criminal outcomes will help to design better responses to these critical failings.

4.15 Work by the Social Exclusion Unit has shown that the 4,000 most deprived estates in the UK experience three times more burglary, 30 per cent higher mortality rates and child poverty three times higher than the rest of the country. Defining deprivation in these more precise ways, drawing on evidence from multiple public sector sources is helping identify and target solutions.

4.16 The Department for Education and Skills has also identified that nearly a quarter of all 16–18 year olds undertake no education or training – 9 per cent are also without work.[41] This is one of the lowest participation rates in Europe and a contributor to the relatively low productivity of the UK. Understanding this specific aspect of the productivity question permits the design of effective remedies and the better targeting of existing training resources. New policies being introduced to tackle this problem include a single advice, learning and support service – Connexions – which will support young people between 13 and 19 in learning and society more generally. In addition, Education Maintenance Allowances have been introduced to counteract the financial disincentives to staying on in education and have already helped to raise participation in education by around 5 per cent in pilot areas.

4.17 Mapping survey data to particular regions or districts can have major benefits, in helping policy makers and administrators identify the key issues facing communities or services. The work of the Intra-governmental Group on Geographic Information (IGGI) has focused on the ability of the public sector to

[40] *The economic and social costs of crime,* Home Office Research Study, 2000.
[41] *Bridging the Gap: New Opportunities for 16–18 year olds not in Education, Employment or Training* (Social Exclusion Unit, July 1999).

improve efficiency, particularly in the context of providing geographically-oriented information to the public. IGGI has developed and published the *Principles and Practice of Sharing and Trading Government Information*, which sets out best practice for public bodies in making better use of the data they hold.

4.18 Good practice in the use of statistical and research data for policy making is constantly evolving. Government departments routinely deposit anonymised versions of survey data sets in the Economic and Social Research Council (ESRC) Data Archive, so that they are available for further analysis by other departments and by the academic community. Samples of anonymised records from the 1991 Census were similarly shared through the Cathie Marsh Centre for Census and Survey Research at the University of Manchester and the centre has gained ESRC funding to support and disseminate the 2001 Census Samples of anonymised records. As the examples in the previous paragraphs show, there are benefits when data from various sources can be analysed together. Government statisticians are looking for ways of making more use of existing data, whether from administrative sources, surveys or the census, for social policy analysis. One route is to match individual records within a secure environment and to produce non-disclosive statistical analyses. Such statistical exercises could provide a test-bed, not only for technical developments in security and anti-disclosure checking but also for public debate about data matching.

More efficient Government, using data to improve value for money and streamline services and to help tackle crime and fraud

4.19 The public sector is also using information to improve efficiency, and tackle waste and error in public services. More efficient public services not only mean saving the taxpayer's money, but also cutting through the red tape to free front line workers to focus on service delivery.

Improving efficiency

4.20 Research suggests that a substantial amount of time can be spent in collecting and verifying personal information. A 1997 study of Information Management in NHS Community Trusts[42] found that information cost a great deal to collect and process – staff spent about 25 per cent of their time collecting and using information. The Audit Commission estimated that information management could consume about 15 per cent of a Trust's running costs, equivalent to £6 million in an average Trust. The Commission further estimated that better data management could secure administrative savings of up to £30 million annually in England and Wales and a further £180 million in clinical time could be released to invest in patient care. One of the aims of the current NHS Information Strategy[43] is to address the shortcomings in data management and so enable health care professionals to focus on their primary responsibilities.

[42] *Comparing Notes: A Study of Information Management in Community Trusts* (Audit Commission, 1997). See also www.audit-commission.gov.uk/ac2/NR/Catal/commun01.htm

[43] *Information for Health: An Information Strategy for the Modern NHS 1998–2005* (NHS September 1998). See also www.doh.gov.uk/ipu/strategy/update/index.htm

Tackling crime and fraud

4.21 Historically, the criminal justice system has suffered from a lack of investment in IT and an agency-specific focus, which meant that very few systems were compatible – for example, some police systems are not compatible across forces. This has resulted in a slow, inefficient and frustrating system for front line practitioners, victims and families of offenders.

4.22 The Criminal Justice Integration Unit (CJIU) and its associated programme – previously known as the 'Integrating Business and Information Systems' (IBIS) Medium Term Strategic Plan – is responsible for the joint initiative between the Home Office, Lord Chancellor's Department and Crown Prosecution Service to ensure better integration of information systems, IT and related business processes across the criminal justice system. CJIU is ensuring that a whole system approach is taken to information systems development across the criminal justice system, and that business processes are designed to take full advantage of the opportunities offered by technology.

4.23 The £1 billion investment over the next 10 years announced in *Criminal Justice: The Way Ahead*[44] will transform and improve the criminal justice system by:

- sharing data to help reduce crime and protect communities;
- improving the management of individual criminal 'cases' for greater speed and efficiency;
- using management information to raise performance; and
- providing a better service to the public.

4.24 Better data use can also improve fiscal efficiency in a number of ways. For instance, it is estimated that fraud throughout the Social Security system is between £2 billion and £4 billion.[45] That total is gradually edging down due, in significant part, to better sharing of data between departments. During 1998/99, information held by the DWP was compared with information held by local authorities leading to identification of 189,000 data inconsistencies and referrals for further investigations. These investigations led to over £149.5 million of benefit savings for the year.[46]

4.25 Reducing fraud and waste can also release resources to focus on primary services – a key element of the NHS's anti-fraud initiative is to release resources to be spent where they matter most, on primary health care. The National Audit Office recently reported that the Department of Health's Counter Fraud Directorate was investigating 484 cases, involving 542 people and with a total estimated value of £18.3 million. In the 2000/01 financial year, over £3 million of fraud was recovered – and a further £4.5 million had been offered for recovery.[47] By targeting fraud and abuse, public services can release resources to be spent where they are most needed.

4.26 Using limited resources more effectively is another way to improve efficiency. The Home Office's Project JUPITER – 'Joining Up Partnerships in the East Midlands Region', now being developed for implementation nationally – is aimed at establishing an information sharing and crime-mapping network for local Crime and Disorder Partnerships. It is geographically based and will provide a regional perspective of crime and disorder trends. Included will be

[44] HMSO, February 2001. See also www.official-documents.co.uk/document/cm50/5074/5074.htm
[45] *The Informal Economy*, Lord Grabiner QC (HM Treasury, April 2000).
[46] *Safeguarding Social Security: Getting the Information we need* (Department of Social Security, July 2000).
[47] *Report of the Comptroller and Auditor General: NHS (England) Summarised Accounts 1999–2000* (National Audit Office, July 2001). See also www.nao.gov.uk/pn/index.htm

the ability to identify areas of strength at local level and give clear identification of areas requiring further support through indicative mapping. The project's main objectives are:

- to facilitate the exchange and mapping of relevant data within Crime and Disorder Partnerships;
- to provide data to regional Government Offices for use by the regional crime reduction director and their team; and
- the linking of Government Offices and central government, enabling comparisons to be made between Partnerships across the country.

4.27 The data can be anonymised and combined with information from a wide range of currently available data sets including those on health, education and exclusion to produce clear and accurate maps of the problems facing the Partnerships and where their limited resources can be used most effectively.

The Anti-Terrorism, Crime and Security Act

4.28 The events of 11 September posed a direct challenge to the UK to ensure that, in future, it is as fully prepared as possible to meet the threat of terrorism. The Anti-Terrorism, Crime and Security Act – which received Royal Assent on 14 December 2001 – is the result of an extensive review of existing legislation to ensure that the UK has the necessary powers to ensure the safety of UK citizens at home and abroad.

4.29 The Act contains provisions to remove current barriers that prevent customs and revenue officers from providing information to law enforcement agencies in their fight against terrorism and other crime. The Act creates a new gateway giving HM Customs and Excise and the Inland Revenue a general power to disclose information held by them for law enforcement purposes and to the intelligence services in support of their functions. This is urgently needed to ensure that known criminals are brought to justice. For example, the provisions of the Act allow for information on a suspected terrorist financier's bank account to be passed to the police.

4.30 The Act also clarifies and harmonises a number of existing gateways for disclosure of information from public authorities to agencies involved in criminal investigations and proceedings. The gateways will ensure that public authorities can disclose certain types of otherwise confidential information where this is necessary and proportionate for the purposes of fighting terrorism and other crime. The Act also gives additional powers to require carriers to collect information about passengers on internal and international air and sea journeys and creates a new power to collect information about goods. Carriers will be required to provide the information to the enforcement agencies. This information can then be shared between the agencies.

4.31 These powers are essential to allow law enforcement agencies to target and track terrorists. Details of the information that carriers will be required to provide will be decided in secondary legislation. The information will also be useful in targeting other serious criminals, such as drug smugglers and people traffickers. In this way, freight information will plug an obvious gap in the intelligence gateway.

Box 4.5: Tracing missing offenders

One of the biggest difficulties faced by the magistrates' courts in enforcing fines and breaches of community sentences is locating 'missing' offenders who have defaulted on payment or failed to complete a community penalty order. The Lord Chancellor's Department has agreed an Information Sharing Protocol with the Department for Work and Pensions (DWP), which enables the courts to check some basic personal information – name, address, date of birth, National Insurance number – with DWP. The scheme was piloted in four courts before national implementation on 1 April 2001. The new arrangements have been welcomed by the magistrates' courts and initial results are most encouraging – DWP provided a new or different address for missing defaulters in almost 60 per cent of the cases referred to them by the magistrates' courts. In around a quarter of enquiries the details held by DWP matched those already known to courts; about 17 per cent revealed no trace of the individual.

Tackling debt and enforcing court judgments

4.32 Data-sharing between agencies can also improve the enforcement of court judgments. For instance, up to 60 per cent of enforcement in the county courts is ineffective because the claimant cannot find the necessary information about the debtor to enable them to make the right method of enforcement. In addition, £47.2 million of fines enforced through magistrates' courts was written off in 1999/2000, much of this through an inability to trace missing defaulters. Sharing information between government departments is enabling the courts to tackle this problem more effectively, as detailed in Box 4.5.

4.33 Debt enforcement can be carried out more efficiently and cost effectively when information about debtors' financial circumstances and assets can be accessed. It is important that government creditors should be able to share a range of relevant information in order to target appropriate enforcement measures and avoid fruitless action which would be unnecessarily costly. Similarly, non-government creditors would benefit from access to this type of data.

4.34 A difficulty experienced by government and non-government creditors alike is the choice of which enforcement method to use. This choice is dependent upon a creditor's knowledge of debtors' circumstances and assets. If this knowledge is based on limited facts, the creditor may not employ the most appropriate enforcement method. Using an inappropriate method may prove to be expensive and may not recover the debt owed, and may also lead to the debtor being subjected to excessive or oppressive enforcement methods.

4.35 If a debtor is determined to avoid payment, creditors may experience difficulties in locating them, their employment status, details of assets and their location. Access to this type of information would help to overcome this difficulty. For example, an attachment of earnings (or in Scotland an earnings arrestment) is one of the most effective means of enforcement for creditors, and least intrusive for debtors, but depends upon knowledge of debtors' employment. It would also help to be able to distinguish

between debtors who are unable to pay and those who refuse to pay, and therefore allow creditors the opportunity to consider whether further enforcement action is appropriate in the circumstances.

4.36 Allowing public bodies to share data and to access information held by third parties – with the appropriate safeguards built in to protect privacy and prevent misuse of the information – would help to deliver a more effective and efficient enforcement system for all creditors. A more streamlined and effective enforcement system would result in a considerable increase in efficiency and substantial cost benefits to government, business and the public. The Lord Chancellor's Department and the Scottish Executive are both considering proposals for action to address the shortcomings in current enforcement practices.

4.37 In summary, for the public, better use of data can deliver smarter public services, more inclusive policies and better value for money. For public services, better data use can lead to better value for money, better targeted services and more effective means to tackle crime, fraud and enforcement of civil judgments. While benefits to taxpayers as public sector 'consumers' are already being realised – customer-focused services that are more responsive, flexible, easier to use and geared towards meeting their needs – more could be done in the future with better data use.

5. OBJECTIVES AND PRINCIPLES – A STRATEGY FOR THE FUTURE

Summary

Public services should pursue the twin objectives of enhancing privacy and making better use of personal information to deliver smarter public services – it is possible and desirable to achieve both.

Achieving the twin objectives requires a much more strategic approach by the public sector. The strategy should be underpinned by four main principles:

- using the data available in the most efficient and effective way possible to achieve goals;
- adopting the least intrusive approach – i.e. where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so, recognising that the protection of privacy is itself a public service;
- wherever possible – and where the benefits of better use of personal data are for the person using the service – giving citizens greater choice in the use of their personal data; and
- ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in the policy-making process of striking a balance between individual rights and the wider public interest.

The strategy requires significant changes in five main areas:

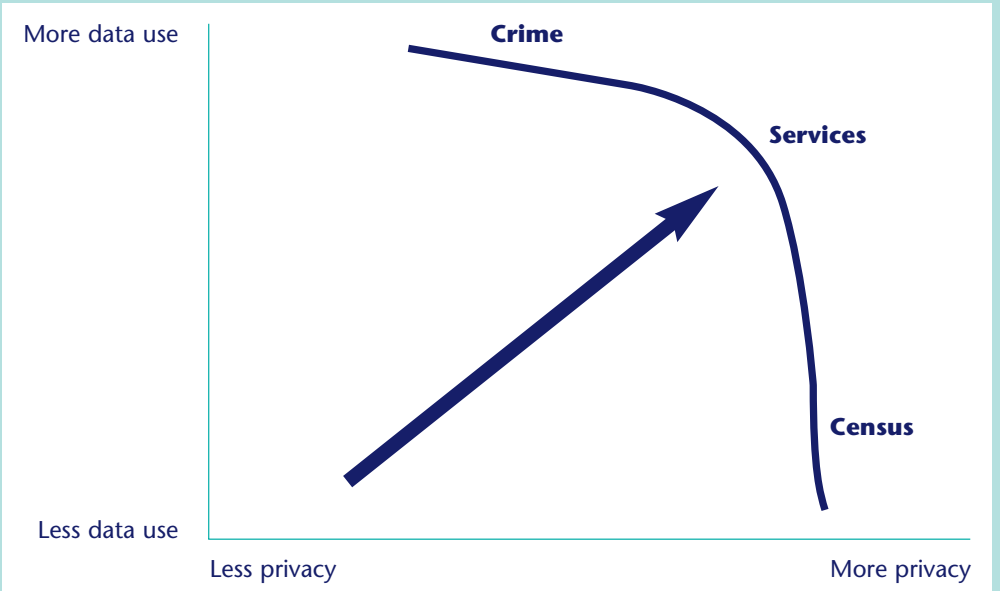
- building public trust and engagement;
- improving data accuracy and reliability;
- using new technologies to support more secure and more joined-up data use;
- modernising the public sector to deliver new ways of managing information and privacy issues; and
- achieving a greater understanding of the existing legal framework and examining options for changes to the ways in which new data-sharing gateways are established in legislation.

Objectives

5.01 In its current practices, the public sector is seeking to find a better balance between privacy issues and the need to improve services. In the future, the rules governing that balance will need to be much more precisely defined along with new ways of doing business. This project has therefore sought to specify the key objectives that should be driving policy and the principles that should underpin it.

5.02 Two objectives should govern policy – enhancing privacy and making better use of personal data to deliver smarter public services. These objectives are *not* mutually exclusive. It is both possible and desirable to achieve both.

Figure 5.1: Privacy and better data use are not mutually exclusive goals



This figure shows the relationship between improved use of identifiable personal data and increased privacy. In some instances – such as crime – it may not be possible to achieve the same level of privacy as in the delivery of other mainstream services. By contrast, in areas such as the census, confidentiality is fundamental to the service. However, in many public services, business processes, technology and system design can deliver privacy and better data use in equal measure – the arrow therefore suggests that, in general, public services should be moving towards the top-right quadrant in their approach.

Where information is anonymised or pseudonymised, the aim should still be to deliver better use of the data with effective safeguards to prevent data misuse. With effective security systems, public services can make improved use of anonymised data without facing the same risks to privacy that use of identifiable data gives rise to.

5.03 In many fields the security and accuracy of personal data can be improved alongside measures to share data between different agencies. But in many cases judgements will have to be made.

Individual rights and responsibilities, and the wider public interest

5.04 The public has both rights and responsibilities in the approach to the use of personal data in delivering public services. Citizens have formal rights and legitimate expectations that privacy will be protected while data are used to deliver tangible benefits. Citizens also have responsibilities, for example to provide accurate data, not commit fraud or other criminal activity, respect civil judgments and so on. And the public rightly expects Government to play a role in ensuring that all members of society respect these responsibilities and that this may involve the use of personal data without consent.

5.05 The use of personal data raises a wide range of issues about the balance between individual rights and the common good. Much of the business of government already involves making difficult choices about how to strike this balance in relation to everything from public health to transport. In the case of privacy too, there are often particularly difficult trade-offs to be made. For example, the individual right to privacy over HIV status may need to be balanced against their safety and the safety of others – for example, prison warders may need to know about a prisoner's HIV status so that they know what to do in an emergency.

5.06 The purpose for which data may be shared means that the balance between personal privacy and the wider public good will be different each time. In considering the wider use of data collected by public bodies, not every case will be clear-cut. This report therefore aims to set out some common elements which should be followed in pursuing the twin objectives of enhancing privacy and making better use of personal data, recognising that in many cases data-sharing will need to occur without the consent of the data subject.

Principles

5.07 As a first step, the strategy to achieve the twin objectives should be underpinned by four main *principles*, derived from the difficult judgements faced by public services:

- the public sector has a responsibility to use the data available to it in the most efficient and effective way possible to achieve its goals;
- in looking at information requirements, the public sector should adopt the least intrusive approach – i.e. where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so, recognising that the protection of privacy is in itself a public service;
- wherever possible – and where the benefits of better use of personal data are for the person using the service – citizens should have greater choice in the use of their personal information to deliver public services; and
- ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in the policy-making process of striking a balance between individual rights and the wider public interest.

5.08 In applying these principles to decisions about the need for increased data use or data-sharing, public services should systematically:

- assess the benefits of the proposed data use/data-sharing in meeting public policy objectives;
- consider alternative approaches to achieving the objectives which do not involve data-sharing and do not impact on privacy;
- identify the costs and risks of increased data use/data-sharing. This should recognise that many of the risks to privacy will be difficult to quantify;
- assess safeguards that would minimise the risks (for example, by use of privacy enhancing technologies); and
- use the accumulated evidence to strike a balance between the benefits and the costs and risks.

5.09 Where increased data use or data-sharing is proposed after this analysis, policy makers should therefore be in a position to explain why the public interest will benefit – and how privacy will be protected or enhanced.

The strategy

5.10 In bringing greater clarity to the balance between privacy and the need to improve services, it is essential that there should be a strong drive for improvement and greater consistency across the public sector. This report sets out the key elements of a strategy for improving services and enhancing privacy.

5.11 The strategy should ultimately ensure that the public sector can use technology and modernised processes to deliver better and faster services, reduce duplication and make public services more convenient and simpler to deal with, cut as much of the administrative red-tape and costs as possible, and tackle crime and fraud – all on a foundation of public trust that information is used in a responsible and secure manner. In this way, service providers will be able to deliver key consumer benefits, such as more '24x7' services, built around consumer needs rather than the convenience of service providers – accessible and flexible services that meet demand quickly, efficiently and accurately.

5.12 The project has identified five main issues for consideration in realising the benefits from better data use:

- there is declining public trust in some public sector organisations and in the way that they handle personal information, and concern about the risks to personal privacy posed by advances in technology;
- the quality of personal information held by the public sector is variable, making better data use and effective data-sharing more problematic;
- there is a risk that the public sector isn't making the most of technological opportunities to redesign core business processes to ensure that services meet citizens' needs and concerns;
- the current approach to the better use of data across the public sector is disjointed and inconsistent, and there are a range of administrative barriers that prevent more effective use of data; and
- there is confusion as to what is and is not allowed within the legal framework. This confusion is exacerbated by a lack of clear and consistent safeguards, without which public trust in better data use is undermined.

5.13 The strategy set out in the following chapters therefore provides integrated solutions to achieve the twin objectives. They are categorised into the main areas of:

- building public trust and engagement;
- improving data accuracy and reliability;
- using new technologies to support more secure and more joined-up data use;
- modernising the public sector to deliver new ways of managing information and privacy issues; and
- achieving greater clarity of the legal framework and consulting on possible changes to improve legislative processes for establishing data-sharing gateways – in line with the twin objectives and principles set out in this report.

5.14 As set out in Chapter 4, public services are already beginning to address the issues listed above. But more can be done. The strategy set out in the following chapters will allow the public sector to make significant advances, providing tangible protection to personal privacy and enabling service providers to realise the benefits for consumers from better use of their data.

6. BUILDING PUBLIC TRUST AND ENGAGEMENT

Summary

While there is huge potential to make better use of personal data to deliver benefits to the public – particularly through the use of new technologies – this will only be realised if the public trusts the way the public sector handles its personal information – which means meeting their rights and legitimate expectations on the protection of personal privacy; and using data to deliver real benefits to individuals and wider society.

At present there is a lack of public trust in the way that the public sector handles personal information, and some concern about the risks to personal privacy arising from the introduction of new technologies.

This chapter focuses on what the public sector needs to do in order to build greater public trust in the handling of personal information. This includes:

- **ensuring clear and consistent principles govern the way personal information is handled right across the public sector – through a Public Services Trust Charter – and making sure that the public is aware of those principles;**
- **ensuring the public has good access to their data and that public services can correct mistakes quickly and efficiently;**
- **ensuring clear responsibility and accountability within public sector organisations for the handling of personal information; and**
- **ensuring the public is aware of their rights and how to exercise them.**

6.01 This chapter is about the actions needed to build public trust in the way that public services handle personal information – failure to take effective action in each of the areas listed below could lead to declining public trust and increasing disengagement. The key is to ensure that:

- clear principles govern the way public services use personal data;
- the public has ready access to their data;
- clear responsibility and accountability exist within public services for the handling of personal information; and
- the public is clear about their rights.

6.02 Data security and effective safeguards against data misuse are also important in terms of securing public trust and are considered separately in Chapter 8.

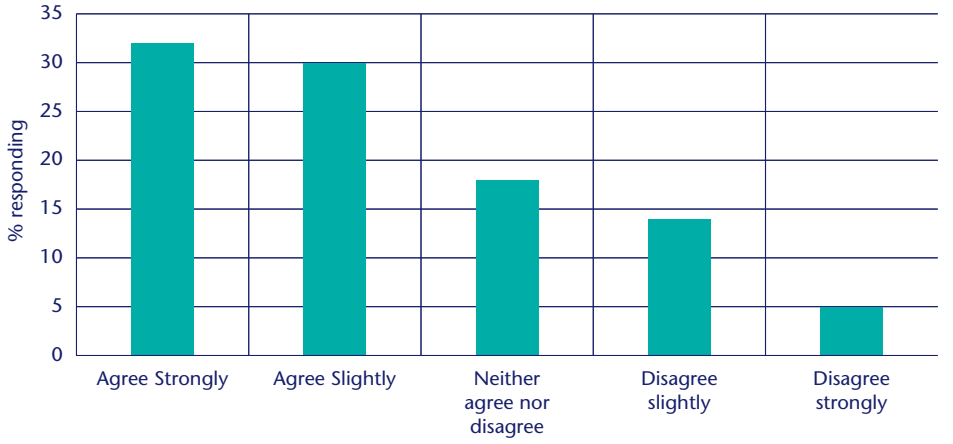
Public trust is vital

6.03 Public trust in the way that public sector organisations handle their personal data – and protect their privacy – is vital to the relationship between the citizen and public services. As stated in Chapter 3, public trust is affected by a number of issues – particularly perceptions of privacy, security and reliability.

6.04 There are concerns that information technology – and the greater use of personal information that it allows – could be a threat to privacy and lead to mistaken identity, inadvertent disclosure of private information and inappropriate transfer of data. There are some signs that the level of public concern about privacy is on the rise – for example, with an increasing proportion of people saying that they regard the right to personal privacy as very important.

6.05 It is clear that if the public does not trust the way that the public sector handles personal information, then it will not be possible to achieve the potential benefits for individuals and for society from better use of that information. In particular, this would put at risk the potential gains for the public from the move to the electronic delivery of public services.

Fig 6.1: "I am worried about how my personal information travelling over new technologies might be used", %[48]



[48] Consumers' Association/IPSOS – RSL, May 1999. Also quoted in *e.gov* (PIU, September 2000).

Clear and consistent principles to be applied across the public sector

A Public Services Trust Charter

6.06 There are already positive examples of good practice in data collection and processing, and several organisations have published guidance – for instance, the National Consumer Council has published a good practice guide on protecting privacy. The guide lists eleven points of good practice, divided under seven headings, which stress the importance of openness in dealing with consumers.

Box 6.1: Protecting privacy – National Consumer Council guidelines[49]

Collecting data

- "Transparency and honesty are fundamental to gaining consumers' trust"
- "Consider how to present information to individuals"
- "Children must be treated as a special case"
- "Obtaining consent"
- "Consider how to tackle changing needs and circumstances"

Complaints and redress

- "Individuals need complaints and redress schemes that are swift, simple, cheap and effective"

Sharing sensitive data

- "Special agreements – or protocols – are needed, setting out how sensitive data will be shared"

Public/private partnerships

- "Certain contracts to deliver services – such as public/private partnerships – need special rules to aid clarity"

Requests to remove, block or correct data

- "Consumer confidence demands that individuals be given the opportunity to challenge information held about them"

Help and information

- "Informing customers about their legal rights and about policy and practice will help to gain their confidence"

Security

- "Think about how to maintain security and confidentiality"

6.07 This simple approach to listing the core principles of data collection and processing can have major benefits in promoting citizens' trust and engagement. The first priority for public services will be to have a consistent approach and principles applied right across the public sector, setting out clearly how personal information will be handled to protect privacy. The approach and principles – a Public Services 'Trust Charter' – are set out for consultation in Box 6.2 below.

[49] *Protecting Personal Privacy: Guidelines for Collecting and Using People's Personal Data* (National Consumer Council, June 2001).

Box 6.2: Draft Public Services Trust Charter – for consultation

This Charter sets out the standards of service that you can expect from public services in the way they handle personal information.

WHAT YOU CAN EXPECT FROM US
In observing the Data Protection Act, public services will aim to ensure that the following principles apply in handling personal information:

Overall principles

- Where you have a choice as to whether to provide us with your information, it is as easy as possible to exercise that choice.
- Your information is only processed without your knowledge where this is necessary for purposes such as national security, public safety, statistical analysis, the protection of the economy, the prevention of crime or disorder, the protection of health or morals, or the protection of the rights and freedoms of others.
- Only information which we actually need is collected and processed.
- Your personal information is seen only by staff who need it to do their jobs.
- Any information which we no longer need is deleted.
- Decisions affecting you are made only on the basis of reliable and up-to-date information.
- Your information is protected from unauthorised or accidental disclosure.
- A copy of any information we hold about you is normally provided on request.
- Any inaccurate or misleading information is checked and corrected as soon as you bring this to our attention.
- Proper procedures are in place for dealing promptly with any complaints that you make.

The principles apply to personal information which we hold both on computer and in some paper records.

Service-specific privacy statements

Wherever we request personal information from you, we will publish a privacy statement for that service which will set out clearly:

- who will see it;
- why they need it;
- what they will do with it; and
- when they will delete it.

We will also tell you:

- how we safeguard your personal information;
- how you can check and correct the information we hold;
- how to pursue a query or complaint; and
- where to get more information.

6.08 The way in which personal information is handled will differ according to the particular issues faced by different public services. The Trust Charter therefore provides a commitment that individual services will develop their own service-specific Privacy Statements. The Charter sets out what information should be included in these statements, so that citizens have a clear understanding of how personal information will be used for that particular service area.

6.09 The Trust Charter – which could be linked to a recognisable logo to ensure that service users could easily identify services which had implemented the Charter – is a development of existing practices. For instance, many websites already have a privacy policy. Similarly, some public services already set out clearly how data are used once they have been collected.[50]

6.10 There is a further, significant step in moving from high-level principles and objectives to specific management practices that inspire public confidence on the ground. To make sure that it happens and goes on happening the public sector will need to:

- develop codes of practice, information sharing protocols (with partner organisations) and detailed management guidance to ensure that the principles are consistently applied (Fig. 6.2 over summarises the relationship and hierarchy from high-level principles down to the detailed management guidance). These should be developed as appropriate in consultation with citizen groups, the Information Commissioner and staff;
- continue developing the policy and technical guidance for securing citizen and business data outlined in the e-Envoy's Security Framework;
- appoint named individuals at senior level to ensure compliance; and
- carry out audits and inspections to ensure that the rules are being followed.

6.11 The Public Services Trust Charter subsumes the prior commitment in the PIU Report *e.gov*[51] and has been developed in partnership with the Office of the e-Envoy. The Office of the e-Envoy will be publishing guidance for applying the Public Services Trust Charter in an on-line environment and will be recommending that it is adopted by all on-line public services, modifying the Security Framework as necessary. The 'e-Trust Charter' can be found on the e-Envoy's website.[52]

Codes of practice and information sharing protocols

6.12 Codes of practice for data-sharing are encouraged in the 1995 EC Data Protection Directive and in the UK Data Protection Act. They are acknowledged as well-established tools for privacy protection because they aim to ensure the implementation of high-level commitments. A code of practice:

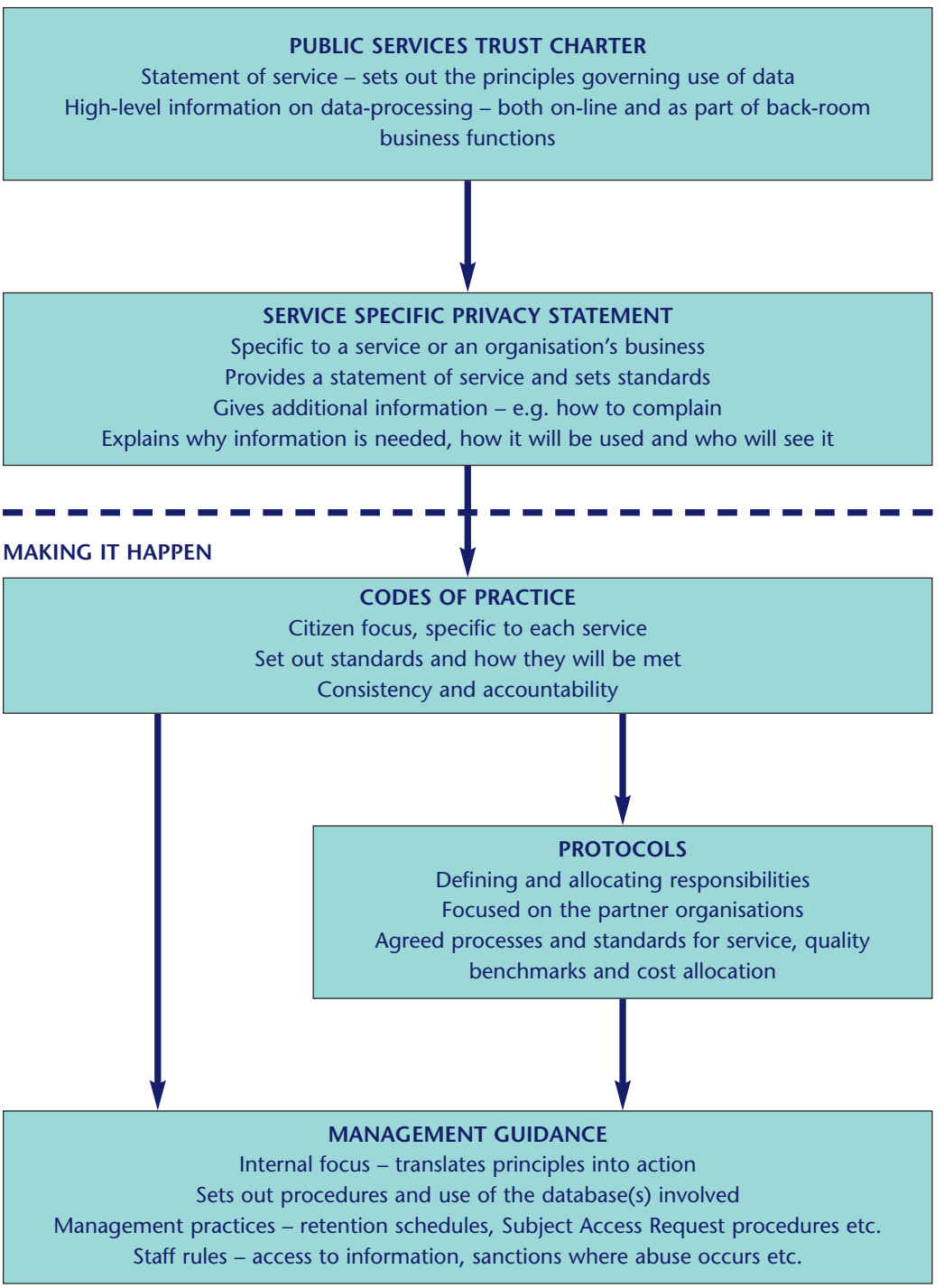
- clearly defines the standards to be met by an organisation and its staff; and
- sets out the steps to be taken in order to meet that standard.

[50] Such as NHS Direct, which covers data and privacy issues in the FAQ section on the NHS Direct web pages: www.nhsdirect.nhs.uk/faqs/nhsdirect.jhtml?noticetype=NHS_FAQ

[51] *e.gov* (PIU, September 2000) Conclusion 12: "The Office of the e-Envoy should develop a Trust Charter for government Electronic Service Delivery in co-operation with the Data Protection Commissioner."

[52] See www.e-envoy.gov.uk/publications/guidelines_index.htm

Fig 6.2: The Trust Charter, privacy statements, protocols, codes of practice and management guidance – inter-relationships



6.13 Well-developed codes of practice will help to support several of the principles outlined in this report. They ensure a degree of openness and transparency, consistency across services and a good degree of accountability by setting out the principles underlying the data-sharing. There are various triggers that may indicate the need for a code of practice, such as the deployment of a new technology likely to have – or be perceived to have – a significant impact on individual privacy, use of existing technology in a new context or use of an existing technology or process known to have privacy implications.

6.14 The Information Commissioner takes a role in endorsing codes of practice, particularly when they aim to explain the steps taken to achieve compliance with the specific requirements of the Data Protection Act (DPA). She has also published guidance on compliance with the DPA and is also empowered to take the initiative, if she sees a pressing need, of calling for a code of practice to be developed.

6.15 Information sharing protocols between public bodies draw on codes of practice, where necessary, but their prime purpose is in defining and allocating responsibilities (e.g. for data maintenance and security), agreeing common subject access measures, agreeing data quality benchmarks and any additional costs. These protocols greatly assist data-sharing by building trust between participating organisations that each is meeting agreed standards. They will be particularly important in new joined-up services that include new partners from central and local government and the private and voluntary sectors.

6.16 Codes and protocols must be flexible – and relevant – in their application. It is important that they are not regarded simply as bureaucratic exercises. Therefore there are no strict requirements for their production. Rather, we propose consultation with key stakeholders, and the provision of guidelines and sharing of best practice by the Lord Chancellor's Department. Public services should make every effort, however, to ensure that codes and protocols embody the right levels of privacy protection.

Management guidance

6.17 Codes of practice and protocols will need to be underpinned by further management guidance, essentially a 'manual' consisting of the department or

Box 6.3: Youth Offending Teams

In implementing Youth Offending Teams (YOTs) as part of the Crime and Disorder Act 1998 (CDA), the Youth Justice Board (YJB) was repeatedly faced with recurring data-sharing questions raised by local agencies. Although the CDA expressly provided for data-sharing across local agencies involved in YOTs, there remained some uncertainty as to *how* that would appropriately be done in order to comply with the Data Protection Act. The YJB solved this problem by drafting specific guidance to help partnerships manage their day-to-day data management issues. Other local partnerships are facing similar issues that could be effectively addressed through standard guidance from the lead central government department.

service-specific instructions on the day-to-day use of data and other management issues. These will be drafted by individual organisations, based on their own internal practices and arrangements and, in time, management guidance should also be accessible to the public, including via the Internet.

Standards in contracts

6.18 One particular area for management guidance is contracts for Public Private Partnerships for the delivery of public services, where the contracting public authority remains the responsible body. The Data Protection Act 1998 requires that where data-processing is conducted by a data-processor this is subject to a written contract addressing, among other matters, data security. Clearly, as regards public trust, it is important that while services may be provided *on behalf of* a public authority, the authority is seen to establish standards and maintain control of, and responsibility for, the process. Public bodies need to ensure that their contractors are aware of, and are able to meet, the expected standards of data management set out in this report.

Recommendation 1: A draft Public Services Trust Charter is published here for consultation. The Charter sets out the guiding principles and key commitments made to the citizen in protecting their privacy and personal data in their interactions with public services. All public sector organisations should look to embody these principles in service-level privacy statements *describing precisely in each case* how personal information will be shared in support of service delivery or research and evaluation, and how individuals can get access to their personal data. In turn, these privacy statements will be key instruments to help inform the public and secure consent where information is shared to support delivery of public services. They must therefore be easily and readily available to the public, where appropriate at physical outlets and websites. To ensure implementation of these privacy principles and undertakings, each service-level privacy statement will need to be embodied in working-level codes of practice and information sharing protocols, themselves underpinned by management guidance. These should also be made publicly available.

6.19 The Government would welcome responses to the proposals listed in Recommendation 1 above, including views on the content of the draft Public Services Trust Charter. Responses should be sent in by 12 July 2002 to:

Paul Henery
Freedom of Information & Data Protection Division
Lord Chancellor's Department
Room 912
50 Queen Anne's Gate
LONDON SW1H 9AT

Fax: 020 7273 2684

E-mail: foiu@homeoffice.gsi.gov.uk

Access to personal data

6.20 In building public trust, it will be essential for public service consumers to:

- know what information public service organisations may hold about them;
- be confident that data can be easily updated or corrected; and
- have confidence that any mistakes that are made will be corrected rapidly.

Information held by the public sector

6.21 The public sector holds vast amounts of personal information, which it needs to deliver key services such as health, education and welfare benefits. But it also needs to ensure that citizens are aware of what types of information each agency holds, in order to enable citizens to make more informed choices about how they interact with public services. Transparency and open government will be essential factors in enabling citizens to make these choices.

6.22 In addition to the right of subject access request under the Data Protection Act 1998, the Freedom of Information Act 2000 places an obligation on public authorities to develop 'publication schemes'. Under this scheme, public bodies should routinely publish information regarding how they conduct their business, their objectives, how decisions have been made and so on. These publication schemes could be extended to cover a statement on information policy, setting out what information is routinely collected to enable the agency to conduct its business, how it handles that information and under what circumstances information is shared with other agencies.

Recommendation 2: In order to provide better information to the public on information held by public services, those public bodies covered by the Freedom of Information Act should consider publishing a statement on sets of data held and data-sharing practices as part of the publication schemes which public sector bodies are required to publish under the Act.

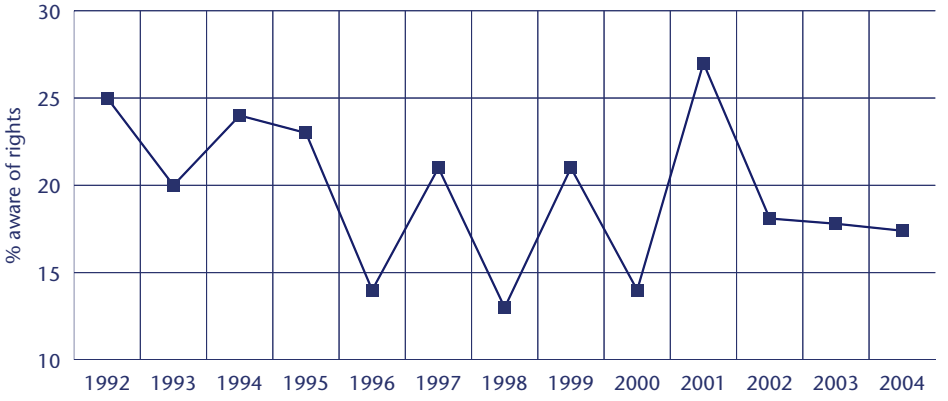
Public access to personal data

6.23 At present, public awareness of the DPA is relatively low, and understanding of its contents and protections is even more limited. In a recent survey, the National Consumer Council found that, while almost three quarters of those polled were aware that they had some rights over what happens to their personal details collected by organisations, only a small number could describe those rights accurately. Around two thirds of those polled wouldn't know what to do if they had a complaint about personal information.[53]

6.24 The Information Commissioner's Office has found through its reviews and surveys that understanding of the DPA provisions and how they protect privacy of personal information is consistently low – although general prompted awareness of the Data Protection Act itself is currently at 71 per cent. In the most recent tracking survey for the Information Commissioner, roughly half of all respondents were unsure of or didn't know their rights under the DPA and between a fifth and a quarter of respondents would not know where to find further information. The peaks in the following chart relate to awareness of the DPA after information campaigns run by the Information Commissioner's Office. The figures for the period beyond 2001 are projections based on current trends.

[53] NCC Press Release, 24 October 2001.

Fig 6.3: Awareness of rights amongst data subjects, %[54]



6.25 The average number of subject access requests (SARs) made to public bodies is reported to be very low. Improved citizen access to personal data could be achieved by making the access procedures easier to use – in particular by providing a clear explanation of rights with a clear point of contact in each public sector body and standard access forms that are in plain language and easy to understand. Public services should also examine less formal procedures for enabling individuals to check their information, focusing on core data such as name, address and date of birth.

6.26 The Data Protection Act sets a maximum chargeable fee of £10 for an SAR to all public bodies, except for education and health records. This figure was agreed as a reasonable compromise between discouraging 'vexatious' requests and enabling the fundamental right to know how one's personal data are used. Cost recovery was explicitly not a principle used to guide the setting of the fee and, in principle, a ceiling on cost recovery remains an important discipline for stimulating efficiencies in departments' information management.

6.27 However, the real value of the £10 fee has declined substantially since it was set following the 1984 Data Protection Act and the new Freedom of Information Act raises additional resource implications for public services: in many cases, the cost to them of provision of, and access to, information is significantly greater than £10 per request. In other areas of public sector information, well-established mechanisms strike a careful balance between access and cost. The Government will need to keep the cost mechanism under review to ensure that a sensible balance is struck between ensuring that everyone, particularly the socially excluded, has ready access to their information and placing a disproportionate burden on organisations.

6.28 Increased use of SARs will provide further incentives and tools for improving data quality, with knock-on benefits for better data use. However, as more regular and informal personal information checks are instituted – such as through the introduction of personal advisers in the employment and welfare services and telephone contact centres in local authorities – formal SARs as defined in the DPA may diminish.

[54] Taken from the Information Commissioner's Annual Report 2001.

6.29 At present, the problems posed by legacy IT and paper-based files make SAR compliance an exacting task for many public services. While there is a clear commitment to making improvements, the costs and scale of the change needed will mean that improvements may take some time to come to fruition. However, in the longer term, new systems and innovative websites such as the UK online portal have the potential to provide a low cost, standard method of quickly accessing and amending personal data.

Recommendation 3: Public service providers should consider ways to improve the public's access to their personal data. As part of this, they should also consider setting clear targets for performance, which should ensure steady improvements against the statutory target for response to information requests,[55] and monitoring performance against these targets.

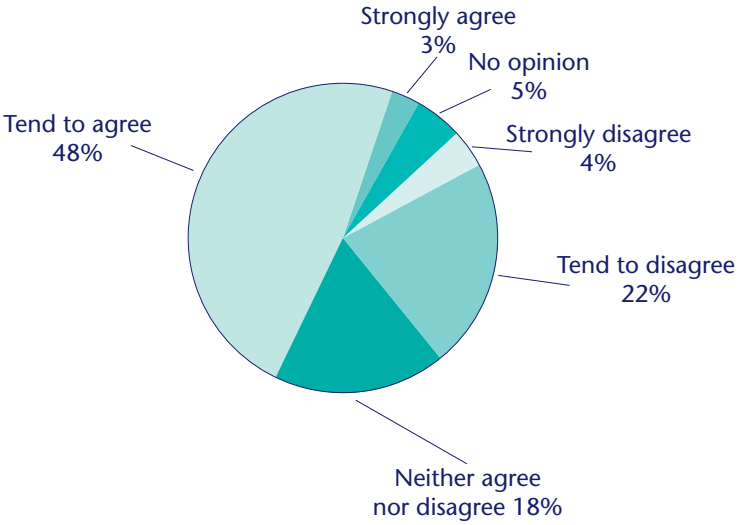
Recommendation 4: Public sector organisations should develop clear explanations of the public's right to access personal data and of access request procedures. This should include a clear point of contact. The information should be provided to customers at point of service, whether on websites or in other publications.

Effective complaints handling

6.30 In the same way that public services need to ensure that consumers have simple and easy access to information held on them, public sector organisations also need to ensure that they have adequate mechanisms to respond to mistakes or concerns raised by the citizen. Private sector experience suggests that effective complaints procedures can turn dissatisfied customers into loyal ones – a complaint, in other words, may be an opportunity to engage with the citizen.

6.31 Unlike access requests, which should be responded to within 40 days, there is no statutory time limit within which errors – including inaccuracy, incompleteness, or excessiveness – should be corrected. Research

Fig 6.4: "Most public services are ready to listen to complaints"[56]



[55] The statutory requirement is that a data controller shall comply with a request promptly and in any event within 40 days.
[56] *People's Panel Wave 5* (Cabinet Office, September 2000). The research also showed that only 33 per cent of respondents were very or fairly satisfied with the way in which their most recent complaint had been handled.

with the People's Panel, published in September 2000, showed that although there was a slow improvement, public services still had some way to go in improving the way they handle complaints.

6.32 In 1998/99 the National Association of Citizens Advice Bureaux noted that they had received around 28,000 cases concerning Housing Benefit where there had been poor liaison between the agencies involved in the complaint – primarily the Benefits Agency and individual local authorities. Such cross-boundary problems will need to be addressed, as more and more public services are delivered by agencies working in partnership. One practical and significant means by which these issues will be addressed will be through the creation of a single, unified Ombudsman body. This will be implemented as soon as the Parliamentary timetable allows.

6.33 The aim for the public sector should be to provide clear information to citizens on how complaints are handled, to have responsive procedures in place, and to respond to complaints quickly. If those procedures do not resolve the issue, there are other mechanisms that could provide citizens with an alternative way to pursue their complaint.

6.34 One possible solution is 'Alternative Dispute Resolution', an umbrella term used to cover a range of processes from facilitated negotiation to binding decision making – processes that can provide faster and more responsive mechanisms for resolving differences. For the public sector a system of mediation under which a complaint could be referred to an independent mediator might be suitable. Such an approach has been employed in the United States.

Recommendation 5: Public sector bodies should examine existing procedures to enable the public to correct their personal information to identify whether procedures can be simplified and improved. They should also consider setting targets for response, and monitoring and publishing performance data.

Recommendation 6: The public should have access to quick and efficient procedures for dealing with complaints about the handling of personal information. Public service providers should therefore consider improvements to existing complaints procedures and new mechanisms for dealing with complaints, including an examination of the potential for adopting Alternative Dispute Resolution procedures.

Responsibility and accountability

6.35 A barrier to citizens exercising their rights can be the lack of a clear first point of contact within public bodies. Some efforts have been undertaken to solve this problem – for example, 'Caldicott Guardians' have been established in all NHS bodies. They are responsible for the procedures governing access to, and the use of, person-identifiable information within the organisation, and the transfer of such information to other bodies. In agreeing local procedures and protocols the Guardians also ensure consistency with any relevant central requirements and guidance. Such innovations could usefully be replicated elsewhere in the public sector.

6.36 A point of contact is important in establishing clear accountability externally,

but there are further measures that can improve accountability and responsibility internally. For example, there are already instances of firm action within the public sector – internal sanctions against staff misuses of data are effective and readily enforced. ATAS is the Department for Work and Pensions (DWP) audit trail system, and prompts Supervisors where information has been accessed inappropriately by staff, leading to investigations where appropriate. In the period April 1999 to March 2000, 214 cases of suspected internal fraud or abuse were investigated – including 20 cases of unauthorised disclosure of information – and 18 staff were prosecuted. It should be noted that DWP employs around 83,000 people – over 80 per cent of whom are employed in the Benefits Agency – and holds records on millions of customers, which are constantly being accessed and updated.[57] The small number of cases of fraud and abuse is therefore a good indicator of the professionalism of public services in handling personal data.

Recommendation 7: All public sector organisations should have a named senior manager with clear responsibility for the handling of personal information. They

Box 6.4: The role of Caldicott Guardians in the NHS[58]

Following the Caldicott Report in December 1997, a network of Caldicott Guardians was established across the NHS. The primary role of the Guardians is to protect patient information. The Guardians are senior health professionals with responsibility for promoting clinical governance within their organisation. They are responsible for:

- agreeing and reviewing internal protocols governing the protection and use of patient-identifiable data;
- agreeing and reviewing protocols governing the disclosure of patient information across organisational boundaries;
- developing security and confidentiality policy; and
- resolving local issues when they arise.

The Caldicott Report also recommended a series of actions to be undertaken by NHS organisations in support of the Guardian:

- develop local protocols governing the disclosure of patient information to other organisations;
- restrict access to patient data by enforcing strict need to know principles;
- regularly review and justify the uses of patient information; and
- improve organisational performance in key areas – such as database design, staff induction, training and compliance.

The Guardian enables good use of information across organisational boundaries, by ensuring that clear protocols govern the exchange of information, ensuring that the organisations involved are aware of legal issues and compliance requirements, and by providing an internal safeguard and check against data misuse.

[57] Social Security Departmental Report (DSS, March 2001). The Department of Social Security is now the Department for Work and Pensions (DWP).
[58] See Health Circular HSC 1999/012, also available at www.doh.gov.uk/confiden/cgmhsc.htm

should also have a clear first point of contact for members of the public on personal data issues. Internal measures to identify and sanction staff for misuse of personal data should be reviewed.

Increasing public awareness

6.37 Public bodies need to ensure that consumers and service providers have sufficient knowledge to participate in debate on specific issues as equal partners and to enable citizens to make informed choices about how to interact with public services. This will raise the profile of the rights enshrined in legislation and ensure transparency in service delivery. Implementing the recommendations above is an important first step, but public services should also maintain an ongoing relationship with service users.

6.38 Research suggests that there is a lack of public awareness of rights and obligations, and also that there is a mismatch between the language of individuals and that of regulators. As with other legally enforceable rights and obligations, it is necessary that there is a precise language and terminology, but plain English should be used wherever possible.

Recommendation 8: The Information Commissioner should continue and expand current activities to promote public understanding and awareness of their rights and obligations. Public services should also promote greater understanding through plain language explanations of DPA and FoI.

7. IMPROVING DATA ACCURACY AND RELIABILITY

Summary

The achievement of the twin objectives of promoting privacy and better use of data depends crucially on the quality of the data available. Inaccurate data both increase the risks to privacy and decrease the ability of the public sector to deliver better targeted, more personalised services. Data quality can too often be seen as someone else's responsibility within organisations.

The available evidence suggests that the accuracy and reliability of personal information held by the public sector is variable, making better use of data and effective data-sharing more difficult, and increasing the risks that mistakes will be made. Furthermore, there are few widely accepted, well understood, quality measures to assess the standard of databases.

New arrangements and incentives are needed to improve data accuracy and reliability and give information management a higher profile within the public sector:

- **agreed standards of how common items of data should be recorded;**
- **better measures of data accuracy and reliability; and**
- **stronger incentives to improve data quality.**

7.01 At present, the reliability of data in the public sector is difficult to determine. Data quality is rarely and inconsistently measured. When it is measured, quality can appear low but the significance is often not indicated. In order to achieve the goals of protecting privacy and delivering better public services, it is essential that public services achieve improvements in the accuracy and reliability of personal information. This chapter looks first at why the issues of accuracy and reliability are important and then at the priorities for action to improve the current position.

The importance of accurate and reliable data

7.02 Quality covers a range of issues, such as accuracy, reliability and 'fitness for purpose'. Inaccurate information both increases the risks to privacy and decreases the ability of the public sector to deliver better-targeted, more personalised services.

7.03 There has been increasing attention given to the issues of data quality in recent years in both the public and private sectors, and evidence is beginning to accumulate about the quality of databases in public services. It shows that the quality of public sector databases is highly variable and, just as importantly, that the criteria and standards used to measure quality vary greatly as well.[59] What it rarely shows is the impact of that quality level on the delivery of the 'primary purpose'. Nor do most data quality assessments do much to inform others, including potential new users, of the possible implications of that inaccuracy for new purposes. Errors that may be insignificant or manageable in the present – in other words, the data may be 'fit for purpose' – may grow in significance if the information is put to a different use.

Box 7.1: The Electoral Register – some aspects of data reliability[60]

At the 1997 general election, the Electoral Register consisted of 44.2 million names and addresses of people in the UK over the age of 18 and eligible to vote in local, national and European elections. But how reliable is it? What do we mean by 'reliable' and how do we assess it?

There are two key aspects to data quality of the electoral register: its *completeness* – the extent to which it fully captures the entire population of eligible voters; and its *accuracy* – the extent to which it has voters registered at their correct addresses. Both are surprisingly difficult to measure.

A number of estimates have been attempted of the numbers of people who have, for whatever reason, failed to appear on the register. It is difficult to make comparisons between data on the general public and the registration returns because they are not based on entirely consistent information. For example, the general population includes foreign nationals not eligible to register as voters. Surveys carried out after the 1991 Census show that non-registration almost certainly rose from around 4 per cent of the eligible population in 1966 to over 7 per cent by 1991. A generally accepted assessment is that some 3–4 million are missing from the register.

Compulsory annual registration has been the means by which the electoral register's accuracy has been maintained. However, with a delay between collection of the new data and publication of the new register, there is a period of thirteen and a half months over which the data degrades – for instance, sample surveys suggest that 10 per cent of people move home in a year. As of February 2001, this particular source of inaccuracy has been reduced by the introduction of 'rolling registration' which will permit electors' information to be updated on a continuous basis.

[59] For example, the electoral register is estimated to have an 'accuracy' level of just over 80 per cent based on a comparison with other reference data sets and surveys; the Police National Computer was found to have an error rate of between 15 per cent and 66 per cent based on the discrepancies between recorded incidents and recorded crime.

[60] Taken from the final report of the Working Party on Electoral Procedures, October 1999.

7.04 More data-sharing has the potential in principle to be detrimental to data quality. For example:

- with wider access and use, external – i.e. users outside the department which originally collected the information – or inexperienced users may create errors;
- with increased external use, there is greater potential to spread errors; and,
- the existence of multiple users may blur 'ownership' of the database and with it the loss of responsibility to supervise database practices and maintain quality.

7.05 Equally, data-sharing and multiple access can, if properly managed, have a positive effect on data quality: more active databases with more users increase the average number of times a single entry may be accessed, checked and validated. As such, errors may be detected and corrected sooner. It is the existence of clear understandings between potential data-sharers – defined and agreed in codes of practice and information sharing protocols – of the basic rules of sharing that will ensure that data-sharing contributes to improvements in data reliability.

7.06 There are three priorities for achieving improvements in data quality:

- introducing basic standards for recording common items of information and for describing and labelling data sets;
- developing methods for measuring the accuracy and reliability of data sets; and
- use of quality audits to act as a diagnostic tool for public bodies and improve public confidence.

7.07 Good management of data entry, if applied consistently across organisations, should also deliver improvements in data quality.

Development of basic standards for recording common items of data and for labelling data sets

Standards for recording common items of data

7.08 Major sources of difficulty in data-sharing arise from some of the most basic information fields, such as name and address or date of birth. For example, it may be difficult to link different data sets to provide a joined-up service using an individual's name for a variety of reasons, such as:

- personal names can be recorded in many forms, for instance using middle names or initials;
- an individual may legitimately be known by a number of different names (for example, using a maiden name in work and a married name elsewhere); and
- the scope for error in data entry or when personal data are first recorded.

7.09 Similarly, different ways of recording a single address can cause difficulties. Standardisation across public services in the recording practices for these and other key fields would have positive impacts for privacy and for more effective data-sharing: fewer mistakes – fewer mistaken identities, fewer false inferences – would address one of the main causes of public concern, as well as improve data reliability and its fitness for use. The Office of the e-Envoy is already working on this problem through the development of XML schemas on the UK GovTalk website.[61]

[61] www.govtalk.gov.uk

Box 7.2: The National Land and Property Gazetteer (NLPG)[62]

The NLPG is effectively a database providing unambiguous identification of land and property through unique property and street reference numbers. It is at the heart of the proposed National Land Information Service (NLIS), which will promote electronic delivery of land and property related services. NLPG project aims are to:

- work towards the delivery of citizen centred services used by local authorities and their partners through the use of a single national address set;
- help local authorities to manage their information to British Standards;
- provide a core address data set for key initiatives such as the creation of electronic voting (based on nationally linked rolling electronic electoral registers) and simplified property searches for conveyancing; and
- develop a standard methodology for updating and collating addresses and working with partners including the Valuation Office Agency, HM Land Registry, Registers of Scotland, Royal Mail and Ordnance Survey with a simple operation framework.

Standards for labelling data sets

7.10 As with any product, knowledge about quality can be imparted through clear labelling. This label – in IT, known as metadata – can inform data users of the nature of the database, its sources, its coverage, its currency, its legal aspects, how data have been validated, and hence its scope and limitations of use. Good metadata practices permit better data management and clear and informative 'labels of content' also discourage unwarranted or inappropriate use of databases.

7.11 There is already some work in hand within government to address metadata issues, but implementation to date has been patchy. More work is needed to embed the principles within organisational practices. The Office for National Statistics (ONS) and the Government Statistical Service have developed metadata guidelines for the major statistical databases such as the census.[63] Similarly, the e-Envoy's Office has produced an e-Government Metadata Framework[64] setting out the principles and guidelines for consistency and clarity in labelling of databases across the public sector. It defines a simple, international standard metadata system ('the Dublin Core') for textually describing a database. This is to be accompanied by a 'pan-Government thesaurus' to create a standard terminology for metadata 'labels'.

Recommendation 9: To improve the accuracy of data, and reduce the potential for mistakes or inappropriate use when data are shared, public services should consider introducing standards for recording common items of data and for labelling data sets (in terms of their purpose, scope and limitations). A simple quality field in which key quality measures are recorded should be included where appropriate.

As part of this, the Office of the e-Envoy should continue to give high priority to progressing the development and

[62] *e.gov: Electronic Government Services for the 21st Century*, PIU September 2000, page 78.
[63] Census Metadata Strategy, Advisory Group Paper (00)03, ONS, 2000.
[64] E-Government Metadata Framework , Issue: 1.0 For open consultation, Cabinet Office, January 2001.

implementation of the Data Standards Catalogue of standardised data fields, giving emphasis in the work to those most commonly used and of most value to data-sharing, such as name and address. This should draw upon the data quality work done by ONS. The Office of the e-Envoy should also continue to give high priority to driving forward the implementation of its recently published metadata standards.

Standards for sharing and managing data

7.12 Databases developed by public services and used within the confines of that service, often by a restricted set of users, tend to be 'fit for purpose' – of adequate reliability for the immediate uses for which they were created. Legitimate but informal and unrecorded practices may develop to contain or correct errors. If databases are to be shared effectively, these management practices, appropriately reviewed and formalised, also need to be shared. Failure to do so could reduce the value of the database to the new user and increase inaccuracies and management costs.

7.13 Since sharing of databases has a tendency to complicate responsibility for maintaining quality, the negotiation of an information sharing protocol can represent a more formal reallocation of responsibilities around new and existing users. Work such as that being done by ONS, the Home Office and the Information Commissioner as a follow-up to the Social Exclusion Unit's report on Better Information[65] to develop information sharing protocols could potentially be replicated elsewhere.

7.14 Public sector organisations should be moving towards an integrated information management infrastructure for all the information they hold, including personal data. The infrastructure should consider key data management considerations, including the reasons for which data were collected; the length of time for which data should be kept; allocation of responsibilities for the upkeep of the information; access controls and restrictions on use of the data; and the means of eventual disposal. As data-sharing arrangements spread, it will be necessary to develop an understanding of these issues across the public sector, and to understand the data flows between and within organisations and how these flows relate to organisational functions. This broad information architecture should also inform the development of future data-sharing proposals.

Recommendation 10: To encourage widespread adoption of such standards, the Lord Chancellor's Department, working in conjunction with the Public Record Office, should facilitate the development and dissemination of model data-sharing protocols and codes of practice as a resource to public sector organisations. This work will need to draw on a wider understanding of the overall information architecture of government, which maps the creation, flows and uses of information sets, establishes criteria for its sharing, retention and disposal, and allocates responsibilities for sustaining access, quality, reliability and safe-keeping.

Measuring the accuracy and reliability of data sets

Methods for measuring data quality

7.15 The measures themselves and the desired or minimum levels are difficult to prescribe – they are subject and user specific.

[65] National Strategy for Urban Renewal – *Policy Action Team 18 Report: Better Information* (Cabinet Office, April 2000).

For increasingly 'active' administrative databases – such as are envisaged for modern government and will be needed to enable e-government – any absolute measures may also become rapidly outdated and themselves inaccurate. Therefore, the most useful indicators of quality are likely to be good metadata – descriptors of the data capture, validation and management processes – from which potential new users can assess the appropriateness of the database for their desired purposes. However, there is important research work being done in the public sector[66] to develop concepts and measures of reliability that will help to develop a more specific understanding of common data quality issues. These different strands of work need to be drawn together and disseminated.

Recommendation 11: Methods for measuring data accuracy and reliability for privacy and data-sharing purposes should be developed to enable public sector organisations to assess their performance and benchmark against others. The Lord Chancellor's Department should draw on and integrate the work already being done in ONS, the National Audit Office (NAO) and the Information Commissioner's Office to develop a body of knowledge and a set of agreed methodologies for measuring and improving data quality.

Auditing for data quality

7.16 Having developed a suitable methodology, the key will be how it is implemented and used. Auditing is a key tool in improving the accuracy and reliability of public sector databases, and audit as a tool is becoming more important in establishing the accuracy of information and how the information is used.

7.17 The quality of public sector databases is currently assessed through a range of different processes and procedures:

- NAO, the Audit Commission and other Inspectorates regularly include judgements on the quality of relevant databases in the course of a study;
- individual service providers and local authorities frequently re-examine their own databases in the light of new policy and operational demands;
- ONS is starting to undertake a programme of quality reviews of all national statistics on a five-year cycle; and
- HM Treasury's Performance Management Review Programme has begun to review the adequacy of departmental information collection and databases for monitoring progress against Public Service Agreements (PSAs).

7.18 The Information Commissioner's Office has published a data protection audit manual, which it hopes will be used by data controllers who wish to test their compliance with data protection legislation.[67] The audit aims primarily to verify that there is a formal, effective data protection system in place. It does so partly by quality assuring the information held – ensuring that it is accurate and up to date, adequate, relevant and not excessive. This provides a good basis upon which to build a more comprehensive methodology for assessing data quality.

7.19 There are substantial numbers of databases in the public sector, so regular or annual audits would impose excessive costs. However, internal audit programmes should, wherever possible, include data quality as a component, and departments with new data-sharing plans should consider using the audit

[66] Such as the recent review of current best practice methodology for data-matching by the Government Statistical Service Task Force – National Statistics Methodological Series No. 25, July 2001.

[67] *Pre-Production: Guide to Data Protection Auditing.* See www.dataprotection.gov.uk/dpr/dpdoc.nsf

methodology as a diagnostic aid to assess the quality of databases for new sharing proposals. A rolling programme of audit by the public audit bodies, focused on the more important or high-volume databases, would also help to focus energies on the data most commonly used in the public sector.

Recommendation 12: Internal and external audits should be used across the public sector to improve data accuracy and reliability. Using the Information Commissioner's data protection audit manual as a starting point, the Lord Chancellor's Department should draw together the strands of work in the public sector to develop a data quality audit methodology. When developing new data-sharing proposals, public services should consider using the audit methodology as a diagnostic tool in order to assess the quality of the data in question.

Public service providers should also consider whether the results of data quality audits, as part of an overall assessment of fitness for purpose, should be included in any consultation on new data-sharing proposals.

As progress is made in implementing the strategy outlined in this report, public audit bodies should also consider giving more attention to information management issues in the public sector, adopting an agreed audit methodology for information management studies they undertake, and publishing data quality measures.

8. MORE SECURE, MORE JOINED-UP DATA USE

Summary

Service providers have always needed to verify the identity of service users, in order to ensure that the user receives the full service they are entitled to and to guard against fraud and error. With the move to joined-up, seamless services, often delivered electronically, identification issues are gaining importance. This is particularly true given the high – and rising – incidences and risk of identity theft and identity fraud. New technologies are presenting opportunities to simplify and streamline public services and improve security and privacy. But they also present new risks that need to be managed.

Internet-based private sector services are raising public expectations of standards of customer service. But there is evidence that the public is often frustrated by the apparent inability of the public sector to meet these expectations – leaving them disillusioned with public bodies' ability to deliver high quality, innovative public services. Technology can help to improve public services, making them more accessible, more flexible, easier to use and more responsive to citizens' needs, and improving the security of the data held to support service delivery.

Effective use of technology can help deliver more secure and more joined-up public services through, for instance:

- development of approaches to technology-enabled authentication and data protection processes – particularly in the e-government context; and
- increased use of smart cards and similar technologies, which can give citizens increased choice in the use of their own information and improve security and personal privacy.

However, technology is an enabler and not an end in itself – the focus must be on the changes needed to deliver benefits to individuals and to society. In meeting this aim, the public sector has an opportunity to redesign core business processes rather than simply bolt on technological solutions to existing services.

8.01 Service providers need to verify the identity of service users, in order to ensure that the user receives the full service they are entitled to and to guard against fraud and error. With the move to joined-up, seamless services, often delivered electronically, identification issues are gaining importance. A number of emerging technologies may help to make interactions with public services simpler, more streamlined and more secure. Technology provides opportunities to improve services to the benefit of citizens, but also presents new challenges that will need to be addressed.

8.02 This chapter looks at these opportunities and challenges, how technology can help to address the challenges and then examines three main areas for action:

- ensuring that data held in support of public service delivery is secure at all stages, and protected by tangible safeguards;
- addressing the challenges posed by the move to electronic delivery of public services for identification, authentication and entitlement, and guaranteeing data subjects' privacy and confidentiality; and
- the use of smart cards and similar technologies, which can give citizens increased choice in their interactions with public services, improve the security of their information and give individuals greater choice in how their data are stored and used.

Opportunities and challenges

Technological developments are presenting new opportunities

8.03 New technology is enabling better data-processing, which in turn will enable organisations to provide better, more joined-up services that are based on citizens' needs rather than the convenience of service providers. IT systems can automatically link records using simple rules, so even where information is held on different databases, this information can be linked to form a 'virtual database' holding all the information relating to an individual and the service they are receiving, enabling front-line staff to answer all but the most complex enquiries by linking related information.

8.04 Technology can provide simple solutions to national problems. For instance, the new National Adoption Register for England and Wales is a single central database holding details of children who need to be adopted and adults who want to adopt. Previously, this information was held by individual local authorities, who often found it hard to find a match within their limited files – regional variations meant that between one in ten and one in 200 children were adopted each year. The register, which began piloting in September 2001, matches children and families based on multiple criteria, such as age, special needs, religion and family background. This simple IT solution to a national problem will improve children's chances in life, cutting the national backlog of children waiting to be adopted.

8.05 Box 8.1 below describes an innovative approach to the issues posed by the move to electronic delivery of joined-up public services. The approach rests on a restructuring of public services, underpinned by the use of greater data-sharing to support joined-up service delivery.

Box 8.1: The 'Reach' project[68]

Reach is an agency established by the Irish Government to develop a strategy for the integration of public services and to develop and implement a framework for e-government. The basic objectives of Reach are:

- to radically improve the quality of service to personal and business customers of the Irish public service;
- to develop a model for the electronic delivery of public services, known as the Public Services Broker, to help achieve that improvement.

Public service customers want to be able to access related services at a single point of contact, so that they can tell their story, prove their identity and give their information on one occasion only, instead of having to go through the same procedure separately for each related service. To improve services in this way, internal public service processes need to be integrated.

Data-sharing is a key to facilitating the seamless delivery of public services – it promotes customer service and efficiency and reduces the need to call for physical documents. However, customers also want assurance that their data are kept securely and that their privacy is respected with clear safeguards in place.

In response to this, Reach is developing the Public Services Broker. The model seeks to balance the need for the maximum availability of data to public service agencies while ensuring the highest level of privacy and respect for data protection principles. The Public Services Broker model involves an integrated approach on three levels:

- a single access point to related services (integration across agencies, services and transactions);
- updated data available in real time and data available for repeat transactions (integration across time); and
- the same data and experience available across the three main access channels – counter, telephone and Internet (integration across channels).

The Public Services Broker model will be based on a hub architecture - hubs at central, sectoral or local levels can be used to exchange data to support common services at the level appropriate to the sector and local need. Sectoral data stores can be supported by central authentication and security services. This means that data captured once can be re-used by other agencies and on other occasions. The individual's right to privacy will be protected by enabling them to know and exercise control over how their personal information is used.

[68] See www.reach.ie

But there are also challenges

8.06 The ease with which information can be linked raises important issues:

- ensuring that the data used are about the right person – guarding against 'identity theft' and preventing error to the detriment of the individual;
- ensuring that the citizen has greater choice in how linked data are used;
- ensuring that the service provider is dealing with the right individual – guarding against fraud – particularly where transactions are on-line; and
- ensuring data are secure at all stages.

8.07 Good systems are necessary to ensure that information can be linked, so that public bodies can realise the benefits in terms of better services for citizens and better value for money. But at the same time, secure systems will be necessary to ensure that data are handled securely and effectively.

Technology can address the challenges

Linking information and making it easier for citizens to use

8.08 Where information is pulled together from different systems, or relating to different services or events, service providers will need to ensure that the linked data concern the right individual at all stages. Where information is pulled together from several different sources, existing reference numbers may be a barrier to better data use. For instance, if driving, welfare and health records were linked, there would be three separate reference numbers – the National Insurance number, driver number and NHS number. People can legitimately have multiple names and addresses, so a common form of identification – an identifier or reference number – can help to link information about the same person.

Authentication and protection

8.09 Increasingly, interactions between citizens and public services are taking place on-line, where it is much harder to authenticate identity. As neither party can 'see' the other or even a signature or other form of identification, traditional methods of identifying individuals will not work. While identification numbers and smart cards can help deliver consumer benefits – including faster, more responsive services – there are also risks of identity theft and fraud, and to personal privacy. Consequently, authentication and security measures are important considerations.

Privacy enhancing technologies (PETs)

8.10 Privacy enhancing technologies (PETs) can enhance personal privacy and give consumers greater control over how their information is used. A number of private sector companies are already designing solutions. For instance, P3P (the Platform for Privacy Preferences Project[69]) – developed by W3C, the World Wide Web Consortium, who also develop standards for the Web – enables users to take more control over the use of personal information. P3P-enabled browsers can read a snapshot of how a site handles information and a user's preferences, enabling users to make a comparison which enhances their ability to make informed choices about how, when and where to release their personal information on-line. P3P does not automatically protect privacy, but enables a better comparison of a website's privacy policy against a user's preferences, thereby facilitating the exercise of choice.

[69] See also www.w3.org/P3P

Public key infrastructure (PKI)

8.11 A public key infrastructure (PKI) has two links with privacy: confidentiality and authentication, both of which increase citizen control over information. First, a PKI can make it straightforward to use a public key to encrypt a message so that only the intended recipient can read it. Second, a PKI can make it easy to use a public key to check a digital signature, which in turn can be used to authenticate identity when accessing personal data over the Internet and which can provide permanent evidence of participation in an electronic transaction, either commercial or personal.

Box 8.2: The Government Gateway – www.gateway.gov.uk

The Government Gateway is the centralised transaction and registration service for e-government services in the UK. Users can sign up for any UK public services that are available over the Internet – the participating departments and agencies administer the services themselves. On completing a registration process, users are able to use a digital signature or a single user ID to send and receive forms, such as tax returns and VAT returns. Users can also assign an agent to act on their behalf for one or more services. The site is secure, and all personal information sent or received via the site is encrypted.

Digital signatures

8.12 The Electronic Communications Act 2000 provides a framework for e-commerce by recognising the legal effect of 'digital signatures'. It implements in part the UK's obligations under the EU Electronic Signatures Directive (1999/93/EC), which aims to provide a common European legal, business and technical framework for digital signatures.

8.13 Digital signature technology involves several concepts that are often confused. They are:

- the private key;
- the certificate; and
- the digital signature.

8.14 The private key is combined mathematically with the data to be signed to produce the digital signature. The same private key applied to different data will produce different digital signatures. Different private keys applied to the same data will produce different digital signatures. The certificate is used by the person at the other end of the transaction to check the digital signature – it contains information that identifies the person who signed, together with that person's public key. The certificate is itself signed – by an entity called a certificate authority. Box 8.3 opposite provides a simple summary of how the system works.

Box 8.3: Secure e-commerce – a summary

Users receive – or, with suitable hardware or software, can generate for themselves – a pair of keys, essentially two large numbers with special mathematical properties. The user keeps one of these keys private and never discloses it. The other can be safely made public, just like a phone number.

Because of the way the keys are generated, information encrypted with the private key can be decrypted only with the public key, and vice versa. So anyone knowing the user's public key can send the user a message encrypted with that key and can be sure that only the user – who alone has the private key – can decrypt it. This provides a high degree of confidentiality.

The user might also encrypt a message – or a digest of a message – with their private key. This cannot provide confidentiality, because anyone who knows the public key can decrypt it. But the fact that they can indeed decrypt it means only that the message must have come from the user – who alone has the only private key that could have created it. This provides integrity and authentication and can also be used as a basis for non-repudiation – the digital equivalent of a signature.

If a sender signs a message with their own private key and then encrypts it with the recipient's public key, confidentiality, integrity, authentication and non-repudiation are provided together.

If one party doesn't know the public key of the other, they might refer to a certificate. A certificate is a computer file containing the value of a public key, along with details that identify the holder of the corresponding private key. A certificate is itself signed. An entity which signs a certificate is called a 'Certificate Authority' (CA). Two public keys – that of the user and the CA – are now linked.

A public key infrastructure is one which links many public keys together in this way.

8.15 New technologies are emerging that promise to deliver the benefits of PKI, but with neither the management overhead of a public key directory, nor the need for prior registration of the intended recipient. One such system uses publicly available information about the addressee – such as an e-mail address – as the encryption key. To be able to decrypt the messages, the recipient would have to prove their identity to a trusted service provider who would then issue that person with their private key. Communications-Electronics Security Group (CESG) are currently working with industry to ensure that public key technologies are developed to a standard that will meet the authentication and privacy needs of citizens, business and public services.

Information security

8.16 While these developments mean that information can be easily linked, that service providers can be sure that they are dealing with the right individual and that the citizen has increased choice over the use of their information, a further key consideration is ensuring the security of the information at all

stages. Internally, IT systems can provide regulated access to information and audit trails that track who has had access to what information and when. In addition, the public sector has defined management practices and staff rules that apply firm sanctions where information is mishandled. But there needs to be further security to ensure that information or identity isn't 'hijacked' and to ensure on-line security.

Improving identification and authentication regimes – biometrics

8.17 Other technological developments have the potential to provide further security assurances for citizens and service providers. For instance, a single reference number or smart card may still be vulnerable if lost or stolen – enabling a fraudster to steal a person's identity. Biometrics are a developing field that may reduce the risk of identity theft. Biometric technology can offer better authentication techniques, ensuring that access to services is better regulated and therefore better managed, and ensuring that resources are not lost to fraud.

8.18 The advantage of biometrics is that the defining characteristics are much harder for fraudsters to replicate, providing the individual with greater protection against identity theft. For instance, recent research at the University of Cambridge found that the chances of two people having iris signatures that are even two thirds identical are one in ten million. The study also showed that if a computer found that only three quarters of a person's iris signature matched the signature it held on file, the chances of this being a false identification were around one in ten thousand million million.[70]

Addressing the challenges

8.19 There are long-term advantages for both citizens and public services if identification and authentication systems can be improved, and if data are used more effectively to deliver more joined-up, secure services. The growing risk and prevalence of identity theft means that individuals need more guarantees for the security of their information, whether in the public or private sectors. Similarly, public expectations of service delivery are leading to a greater proliferation of channels for accessing services, through the Internet, digital television and telephone call centres as well as traditional face-to-face interactions. The diversity of channels of access is increasing the demand for joined-up service delivery, and a greater need for standardisation of systems and interoperability to ensure services are as seamless as possible.

Security and safeguards

8.20 While technology is enabling better and more innovative uses of data, it also gives rise to new risks. Public bodies need to provide firm assurances that information held in the public sector will be secure, and accessed only by authorised personnel and only for specific reasons. Information needs to be protected from two potential threats. These are:

- protection from external access – for instance by hackers – through use of continually updated and strengthened security measures; and
- protection from data misuse through use of safeguards – controlling who can see or use the information, and keeping a detailed history of who has accessed what information for what purpose.

[70] See www.pubs.royalsoc.ac.uk/proc_bio/proc_bio.html

Security against external threats

8.21 The e-Envoy has noted that trust is a significant factor holding people's use of the Internet back.[71] Some of the key issues that public services and industry are currently tackling include:

- protecting children from unsuitable content on the Internet;
- safeguarding the interests of on-line customers and reducing the scope for on-line fraud;
- combating the use of the Internet for criminal activity; and
- protecting the security of on-line information assets.

8.22 With the rise of e-commerce and e-government, the scope for unauthorised data access and misuse is increasing. Governments around the world are significant targets for hackers breaking into systems from the outside and several hacker groups specialise in targeting government websites around the world. UK government sites are no exception. While no site is completely hacker proof, there are security measures and standards in place to ensure as high a level of security is maintained as possible. UK sites conform to the CESG standards, a series of over 20 standards that set out the main security requirements for information held in the public sector. In consequence, the vast majority of hacking attempts on UK sites are ineffective.

8.23 Many privacy invasions come from security failures, whether in terms of information held on- or off-line. Hackers can occasionally gain access to personal information held on websites, and there have been some well-documented examples of such security lapses in the private sector. This has historically been less of a problem for public services, as little business has been conducted over the Internet. However, with the target of providing 100 per cent of government services on-line by 2005, Internet security will become ever more important for public services – government departments are therefore in the process of adopting ISO17799 as the standard for Information Security Management.

8.24 Security is also an issue for public sector staff who have access to personal data – some individuals or companies try to call GP surgeries or Benefits Agency offices to try to find out information about someone. Public services can receive thousands of such calls over the course of a year – while some callers have legitimate reasons, such as attempting to trace an old family member or friend, the majority of requests are for more malicious purposes. Operational policy is to decline such requests as disclosure of personal information would be a breach of public bodies' duty of confidentiality to citizens.

Recommendation 13: The public sector should at least match best practice in the private sector for information security. As part of this, the ISO17799 standard and its associated processes should be adopted across the public sector to provide privacy safeguards. The Office of the e-Envoy and the Communications-Electronic Security Group should continue actively to monitor the development of new technologies and safeguards which could enhance the protection of personal data, building on the existing Security Framework and the e-Government Interoperability Framework.

Internal safeguards and controls

8.25 Citizens need confidence that public services are taking internal security measures just as seriously as external security. As such,

[71] *UK online Annual Report* (Office of the e-Envoy, September 2000). See also www.e-envoy.gov.uk/ukonline/champions/anrep_menu.htm

the public should have confidence that public services are taking steps necessary to control access to their information and keep track of who has accessed it.

8.26 Access controls are one tool for protecting personal data from misuse and audit trails are important tools for both citizens and for public sector bodies in managing information. Access controls are methods to control who has access to an IT system at all, and then who has access to particular types of information or information about particular individuals or groups of individuals. For instance, a receptionist in a GP surgery needs only to have sufficient information to confirm name and address and NHS number, in order to confirm that a patient is registered with the surgery. The GP or a nurse would, by contrast, need to know more information about medical history – although the level of detail can again be controlled.

8.27 Audit trails can be used to track what data have been accessed, who has had access to the data and whether information has been changed or exported. Computer programs write information to a special file known as an audit file when certain operations are done. These files are checked regularly by supervisors and system administrators, who look for unusual or failed operations. If a member of staff is subsequently suspected of browsing information they have no need to see, a complete record of what they have done is available. In addition, systems can flag specific files so that any time they are accessed, the supervisor is informed that the file has been accessed, who has accessed the file and exactly what information has been accessed.

8.28 Systems that hold personal data are records management systems and should be subject to stringent information management controls appropriate for their content. This includes controls on the ability to access, change or extract personal data, and recording of all significant actions taken within the system. Corporate information and records management systems provide these kind of facilities, so that data can be used flexibly when it is appropriate to do so, and restricted when it is not. One of the first steps in designing information management practices is to determine the specific access rights which individuals and groups have in relation to categories of data, and then to build in a mechanism for mapping and managing the interaction between the two. Access controls and audit trails are methods used to put this management into practice across organisations.

8.29 To help public bodies accomplish this, the Public Record Office has produced guidance and functional systems requirements for the effective management of corporate records, and evaluates systems that can support this. These include requirements for the management of personal data, the control of access, and auditing mechanisms which software systems must support; and guidance on the policies and procedures to be operated by those using the systems. Principles apply as much to systems holding electronic documents as to transactional databases.

8.30 The box opposite describes how safeguards are used in the health care system in the Netherlands. The system shows how privacy can be enhanced by small changes to the design of a standard database without any negative impacts on service delivery.

Box 8.4: Enhancing the privacy of patients in the Netherlands

Meerkanten is a large psychiatric hospital to the east of Amsterdam. The hospital has 22 satellite locations, including out-patients' clinics, day-care centres and so on, all networked onto the main computer system. Meerkanten was the first of the 9 psychiatric and 16 general hospitals in the Netherlands which use a privacy-enhanced database system for patient records called X/Mcare.[72]

Each patient in the hospital has a chief psychiatrist. The requirement was that in general no one except the lead psychiatrist could access all the information about a patient; but there had to be a facility for emergency access when the lead psychiatrist was not there, for administrators to access some information for administrative purposes, but without having access to clinical data, and for researchers to see details of symptoms, diagnosis and treatment plans, without being able to identify the patient.

In broad terms there are three main elements ('domains') of patient data in the system which are kept separate: (1) identification data, i.e. patient name, address, local patient reference number etc. also an encrypted version of the carer-identification number of the psychiatrist in the lead for that patient; (2) carer information such as name, unencrypted local carer number; and (3) clinical data, i.e. symptoms, diagnosis, treatment plan including drugs prescribed etc.

The lead psychiatrist can link the three domains. Emergency linking by others is also possible when the lead psychiatrist is not there, but this leads to an entry being written in an audit file. This file is checked regularly.

8.31 The Information Commissioner's Office and the University of Manchester Institute of Science and Technology Department of Computation are also working on a 'Development of Guidance on Data Protection in Systems Design' project. This project has identified the Data Protection Act (DPA) issues that are relevant to systems design, and is producing guidelines for systems development to improve compliance with all eight DPA principles, and make responses to subject access requests faster and easier. This plain language guidance for systems designers and developers, plus practical advice on integration with existing system standards, will help organisations to 'build in privacy' right from the start.

Recommendation 14: Public sector organisations should require information and records management systems to support best practice in ensuring internal security against possible misuse of personal data, and in managing and controlling access to that data. They should ensure that personal data are held in systems which follow best practice in managing access to information held in the system, and in providing audit trails which record information about who has accessed, or carried out operations on, the data. These principles should be applied to new system design.

[72] X/Mcare, the hospital information system for psychiatric hospitals, and X/Care, the hospital information system for general hospitals, are products from McKesson HBOC. The patents on the database concept, known as the 'Secure Database Environment', are held by ICL.

Identification and authentication

8.32 As noted in Chapter 3, issues around identification and authentication are moving higher up the policy agenda, partly prompted by the move to services delivered by partnerships of service providers and partly by the growing risks and prevalence of identity theft. It is unlikely that there will be a single solution to this complex problem, as identification and authentication remain key considerations throughout the lifetime of an individual's interactions with a particular service – from initial application onwards.

8.33 The considerations start with identifying the individual and making sure that they are who they say they are, by checking historical or biographical data held elsewhere about them – such as employment information or data held elsewhere in the public or private sectors for other services – or checking existing forms of identification such as a passport. Each time the user returns to use the service, similar checks need to be made to ensure that the individual receives the full service they are entitled to and to reduce the risks of fraud and error. This can be streamlined through the use of an identification system specific to the service – such as the card and PIN number individuals use in many bank transactions – but even these are not fully secure.

8.34 Government clearly needs to consider identification and authentication issues in the round, building on technological advances, such as smart cards and biometric technology, and considering – in line with the strategy set out in this report – the identification needs of public services and the security and privacy concerns of individuals. Several different models are available for consideration, and each will need to be considered carefully and in consultation with service users. Proposals should also be developed in line with the Analytical Framework set out in Chapter 9 and the Annex to this report.

Recommendation 15: The Government should give further consideration to the broader issues of identification and entitlement to services in the round.

Smart cards

8.35 Smart cards – essentially plastic cards with a chip embedded into the card – can have many functions, ranging from a simple key that enables the user to unlock data to a card that actually holds data file(s). Some cards are intended to store quite large amounts of information, and even money when an 'e-purse' is present – they can also be used for a range of different applications. Others are intended simply for authenticating identity and controlling access to computer systems.

8.36 Many people are used to carrying around credit cards and other similar forms of identification, payment or loyalty cards – often several at once – which can work across organisations or are specific to a service or provider. A similar principle can apply to smart cards – they can be specific to a service, or cover a group of services, and they are held by the service user, who is therefore able to exercise some choice over how and when they are used.

8.37 There are a number of current initiatives which make use of smart cards:

- the DfES Connexions card for young people[73] will facilitate the collection, storage and use of data on 13 to 19 year olds, enabling the better targeting of help where it is needed, and to tailor responses to individual needs. The card will also be linked to shop discounts, enabling the

[73] See www.connexions.gov.uk

teenager to store credits which they can subsequently spend;

- the NHS is currently looking at the potential use of smart cards in its Electronic Patient Record (EPR) and Electronic Health Record (EHR) projects. The EPR would be a short-term store of core personal and recent medical data, which the patient would be able to release to NHS professionals as appropriate. The EHR would be a longer-term medical history. The key change is that the card holder carries their medical record, and so has greater control over who has access to their data; and
- a range of local government and other projects also envisage the use of cards to carry personal information, and which also include public key cryptography functionality. Such projects include:
  - the Wales Information Society project;
  - projects being run by several local authorities;[74] and
  - public transport systems.[75]

Box 8.5: Bracknell Forest Borough Council smart card[76]

Bracknell Forest Borough Council has set up a smart card project called 'The Edge', which builds on a successful loyalty card scheme – 18,600 residents have taken up the loyalty card since September 1999 and more than 100 retail outlets offer cardholders discounts of up to 20 per cent. The council is extending the card's services to meet a variety of purchasing needs and to develop the card into a multi-application, multi-user smart card.

Alongside the existing loyalty schemes involving bus and transport passes, preferential citizen fares and secure citizen token access to web-based systems run by the Council, it is envisaged that the card will be used for:

- cashless school meals;
- Connexions – the Council is running one of the pathfinder schemes;
- an e-purse – including for car park payment;
- library membership and payment; and
- general licence and membership.

The smart card is encoded with the applications and digitally encrypted against fraudulent use. Each application is also fire walled so that each provider cannot access information that it is not authorised to see. Card use is recorded at a reader in each application and uploaded to a central database, which acts as a clearing and settlement system for the e-purse and stores usage data. This also enables the Council to better see how their services are being used and target spending more effectively. In this way, the smart card ensures that the Council can add value to the local community, provide safeguards against fraud, secure efficiency gains and enable better auditing of expenditure.

[74] For example, Aberdeen, Nottingham and Sunderland, as well as Southampton's Smart Cities initiative: www.smartcities.co.uk/index.html See also Box 8.3.

[75] See www.thetube.com/content/aboutus/partner/prestige.asp for details of London Transport's 'Prestige' project to introduce contactless smart card ticketing.

[76] See also www.bracknell-forest.gov.uk

8.38 The Office of the e-Envoy is developing a Smartcard Framework for consultation that will set out core principles for the development of future smart card schemes. The Framework focuses on core principles, such as data transparency – ensuring that cardholders have access to the information that is held on the card – and consent – addressing the question of choice over whether to carry a card or not. Future smart card schemes will need to be developed in accordance with these principles.

8.39 Overall, smart cards and similar technologies can deliver key benefits – greater individual choice in the use of personal information and hence greater privacy, increased efficiency of back-office processes by enabling easier linking of records, and greater security by enabling more secure identification of an individual and reducing the risk of identify theft. As such, public services will need to ensure that they are positioned to enable the realisation of these benefits for citizens.

Recommendation 16: Government should develop a programme of smart card demonstration pilots in specific service areas, in line with the Framework being developed by the Office of the e-Envoy – including consideration of the importance of giving cardholders access to the data held on the card. The Office of the e-Envoy should work with service providers to ensure that a sufficiently broad range of markets and functions are tested and to ensure that interoperability is a key component of system design. This will increasingly allow citizens to make their own choices on what information – covering both the public and private sectors – they carry on their smart cards.

Authentication and protection

8.40 The pace of take-up of PKI and other technologies has been slower than expected to date. Public services face a number of choices, including whether to accelerate the market or to vigorously promote one set of solutions. A series of significant public sector pilots could help to encourage further development of new technologies and further innovation.

8.41 In order to avoid stifling innovation, the Office of the e-Envoy has refrained from selecting a single 'winning' product or technology. However, the pace with which markets are adopting these solutions is not matching the pace of technological change. For instance, while digital certificates are already available from the private sector[77] take-up has been lower than expected. One consequence of this has been that innovative public services have been constrained in their choice of methods for authenticating customer identity. For instance, the Inland Revenue was forced to choose an alternative method for electronic filing of self-assessment tax returns.

8.42 Other countries are moving ahead of the UK in PKI – governments, including Australia, Austria, Belgium, Finland and the Netherlands,[78] are considering or have decided upon action to create a national PKI. However, there remain issues to be resolved – ranging from technological building-block issues to legal liability issues – to ensure that PKI is a secure and useful consumer tool. Government will need to be involved in further development work and market testing to aid the future development of authentication tools as consumer instruments.

[77] For example, from Viacode: see www.royalmail.com/atwork/viacode

[78] See: www.ogo.gov.au/projects/publickey/index.htm (Austria); www.fineid.fi (Finland); and www.pkioverheid.nl/informatie/index.html (the Netherlands)

Recommendation 17: Authentication technologies have the potential to enable public services to provide high levels of security for personal information and to ensure accurate electronic identification and authentication – which in turn will facilitate the realisation of consumer benefits in public services. Given the relatively slow pace of private and public sector development of these tools, the e-Envoy should assess the costs and benefits of increased government involvement in the development of authentication technologies. Potentially, a series of significant public sector pilots – for instance, giving civil servants a smart card or similar device that could be used to create digital signatures at work and which could be taken home for the same purpose in their life outside work – could encourage swifter development of consumer tools. These pilots could test the functionality and infrastructure necessary, and encourage interoperability with the private sector.

9. MANAGING INFORMATION AND PRIVACY

Summary

The public sector is already undertaking major change to improve services to citizens. Improving the public sector's approach to the issues of privacy and information management is an essential part of this change programme if the potential benefits to individuals and society are to be realised.

In order to achieve these aims, this chapter sets out key recommendations:

- **organising public sector bodies to deliver a more integrated approach to the wide range of issues connected with the management of information and knowledge;**
- **ensuring a more consistent and transparent approach to decision making on data-sharing and the balance between individual rights and the common good;**
- **greater strategic direction and effective co-ordination;**
- **increased training and professionalism in information management; and**
- **better incentives for public bodies to both protect privacy and make effective use of the information they hold.**

9.01 Managing information is central to the business of government, and will be increasingly so as government moves beyond the 2005 target for all services to be available electronically.[79] While compliance with Data Protection Act (DPA) and Freedom of Information Act (FoI) responsibilities requires better information management techniques, there are also more systemic benefits such as a stronger consumer focus and better strategic and long-term planning. Modernising the way the public sector manages information will entail an integrated management approach to information issues within public sector bodies, more consistent decision making across public services, and effective co-ordination.

Integrated management approach to information issues

9.02 Information management is increasingly a core function in service delivery – as an enabler of more efficient services and as a means to ensure that personal information is handled fairly and professionally. But not all public sector organisations are fully geared up to the demands placed on public services by increasing public expectations and the changing legal framework. This section therefore sets out some key functions that departments and other public sector bodies will need to take on, and the structures and tools that will help ensure consistent good practice across the public sector.

9.03 There is a growing number of new information management-related roles in public sector organisations; in addition to Data Protection Officers, there are now Information Asset Register Officers, ISO17799 (computer security standards) Champions, Freedom of Information Champions and e-Champions (formerly known as Information Age Government Champions). There are also, of course, the longer established but still relevant functions of departmental librarians, public records managers and statisticians.

9.04 Although some central departments, such as the Office for National Statistics (ONS) and Department for Transport, Local Government and the Regions (DTLR – see Box 9.1 overleaf), have recently established Information Management Directors to combine at board level many of these responsibilities, in many cases these roles remain separate from each other and from the strategic planning and policy-making areas of the department. There is a similar situation in local government, though generated less by directives for champions from the centre and more by a decentralised approach to information management.

9.05 There is a need for public sector organisations to take a more integrated approach to information management – to move from a position where privacy and information issues are often dealt with at lower management level with a compliance mind-set to one where privacy, information and knowledge are integrated with considerations of customer relationship management and business design (including e-business action plans). One option for public sector bodies is to develop the role of a 'Chief Knowledge Officer' (CKO). The CKO would ideally be a board level official who would not only oversee compliance with the DPA and Human Rights Act (HRA) and implementation of the FoI, but also draw together business planning – including e-business action plans – and strategic planning, technology, and other areas to ensure integration of data issues into mainstream decision-making processes.

[79] Also relevant is the requirement that all central government organisations be in a position to reliably manage their electronic information as corporate records by 2004. The Public Record Office is leading this work.

Box 9.1: An integrated approach

In the DTLR, the Director of Strategy and Corporate Services brings together a range of linked functions, including:

- general knowledge and information management issues;
- Data Protection and Freedom of Information;
- modernising public services – including support for DTLR's Consumer Champion;
- electronic records and document management;
- the DTLR Intranet, Electronic Briefing System and Knowledge Network;
- ICT systems and services; and
- the Department's e-business action plan.

In a personal capacity, the Director is also e-Champion and Freedom of Information Champion.

Box 9.2 opposite sets out the range of possible functions that could fall within the CKO's remit, whether through direct line management or matrix reporting.

9.06 In time, public sector organisations should look to take an increasingly integrated approach to these issues – so that the CKO's responsibilities take in more of the functions in the middle and right hand columns in Box 9.2. Organisations will need to consider how quickly to integrate functions and to what extent the CKO should take on the e-Champion role, in the light of existing organisational structures and skills available.

9.07 It will be important to ensure that roles add value rather than simply install an additional layer of bureaucracy. Public sector bodies will therefore need to consider the functions that are already carried out by Data-Protection Officers and e-Champions and how these fit with the possible functions of the CKO.

9.08 As leaders within organisations, CKOs will need to be properly trained and adequately supported. This might suggest a core team of professionals in each of the main areas. In smaller organisations, the level of support would need to be a flexible reflection of what would be necessary and desirable against the available resources. Clearly, a 'one size fits all' approach will not be possible – some public bodies are relatively small and may not be able to devote the necessary resources to information issues. At the same time, organisations will need to mobilise themselves to ensure that they are able to meet increased demands for information about their activities, the information they hold and how individuals can exercise their rights.

Box 9.2: Chief Knowledge Officer – range of responsibilities

Increasing integration

- DPA/HRA compliance
- FoI
- Data standards
- Data-sharing protocols
- Records and information management

- Business design and e-business action plans
- Customer relationship management
- IS/IT strategy

- Analytical, research and statistics services
- Research and evaluation to feed into decision making

The wider public sector

9.09 Local authorities and other public bodies should also consider the value of the CKO role, though again there may be legitimate resource constraints on smaller organisations. Local authorities, supported by the Local Government Association (LGA), the Improvement and Development Agency (IDeA) and the Office of the e-Envoy, have already begun to develop Implementing Electronic Government Strategies (IEGS).[80] This work has involved the creation of e-government champions along the lines of central government e-Champions.[81]

9.10 Local government has a long-standing tradition of professional networks through which it shares knowledge and best practice. While the majority of local authorities may not be able to implement the CKO model in full due to resource constraints, some of the larger authorities could be able to do so. Authorities should also consider whether pooled resources could create a shared CKO function across partner authorities.

9.11 More generally, IDeA is well placed to take on a co-ordination role for local government, providing a source of advice and best practice for organisations. IDeA is also well placed to forge close links with the Lord Chancellor's Department's (LCD's) role in relation to co-ordinating those aspects of the strategy which relate to local government, although in considering how the strategy applies to them, local authorities will want to give priority to meeting existing requirements, including implementation of the Freedom of Information Act. In addition to this, the Cabinet Office (CO), LCD and DTLR will need to address with key stakeholders the outstanding issues around the exchange of information between central and local government.

9.12 The links between this report and local government will also be affected by:

- the Local Government Online (LGOL) programme, which makes £350 million funding available to councils through DTLR. In implementing their own LGOL-related programmes, local authorities should incorporate as far as possible the recommendations in this report;
- the forthcoming publication of the national LGOL strategy by DTLR and its partners, which will need to include

[80] *Local e-government now: a baseline for measurement*, April 2001, SOCITM and IDeA, 2001.
[81] Separate arrangements apply in Scotland, Wales and Northern Ireland where the devolved administrations are taking forward local co-operation on e-government.

appropriate local government engagement in the conclusions; and

- Audit Commission participation in the development and use of measures and audit methods – including in the five yearly Best Value audit of councils' implementation of the e-government agenda.

9.13 In approaching information management, and in developing the CKO role, the wider public sector will need to build on existing good practice – such as Caldicott Guardians in the NHS – to ensure that information management is at the heart of business design.

Recommendation 18: Public service bodies should consider integrating the functions set out in Box 9.2 above, including through an evaluation of the appointment of a board level Chief Knowledge Officer as a means to ensure integration of information issues into decision-making processes. Ideally, Chief Knowledge Officers would be responsible for integrating, over time, the disparate functions of legislative compliance and business planning.

9.14 As more and more public services are delivered in partnership through electronic channels, traditional departmental boundaries will become blurred. In these cases, organisations will need to ensure that accountability and responsibility for the service are clearly set out. This could, for instance, mean the CKO from another department taking responsibility for the design of a core service delivered – at least in part – by another organisation.

Consistent decision-making across public services

9.15 A strategy for advancing both better privacy and better data use needs to be underpinned by a clear framework for decision making on privacy and data-sharing issues. Whenever the costs, risks and benefits of a policy approach are new, diffuse, indirect or occur over different time scales, they are not easily quantifiable or comparable. Standard cost-benefit techniques are incomplete for the purpose. It is important, therefore, to have a clear process by which the costs and benefits can be identified and described. This process should be applied in advance as part of policy and systems design.

9.16 An Analytical Framework[82] has been designed to aid this process. It attempts to condense the decision-making process into its basic steps – at each step, it attempts to group into discrete types the different benefits, risks and costs that may arise. It aims to give conceptual clarity to each of the different costs and benefits and should also help in identifying particular gaps in knowledge and methods.

9.17 This approach helps with the appraisal of a new policy where quantitative evidence is lacking, particularly as it will:

- **ensure consistency in considering privacy impacts.** This is important in itself, for reasons of analytical rigour and clarity, and for reasons of public confidence – ensuring that public services are visibly committed to consistency and clarity;
- **integrate privacy costs and risks into a wider cost-benefit analysis.** This signals the intention to give to privacy considerations a weight in the appraisal process equal to traditionally more quantifiable measures;

[82] See also the Annex to this report, and Annex D on the PIU web pages www.piu.gov.uk/2002/privacy/report/index.htm

- **ensure an opportunity for unfamiliar, unanticipated and indirect costs and benefits of data-sharing to be identified.** The framework helps to ensure that difficult cost issues are examined in full and should help to stimulate the collection of evidence of benefits, costs and risks and contribute to a more developed appraisal methodology;
- **contribute to transparency.** The systematic approach aims to facilitate understanding of the decision-making process; and
- **constitute a more systematic assessment of proportionality.** The experience of challenges under the ECHR to date suggests that weight is given to evidence of genuine attempts by governments to assess the appropriateness of their actions.

9.18 A potential component of the Analytical Framework is a Privacy Impact Assessment (PIA), which is already in use in countries such as Canada and New Zealand. PIAs are outward-facing documents that set out the benefits and the risks, and the organisation's conclusion based on these assessments – they are used to promote an informed and open dialogue between public bodies and service users, based on shared knowledge of the opportunities, benefits and risks.

Recommendation 19: To promote more consistent decision making across public services on privacy and data-sharing issues, the Privacy and Data Use Analytical Framework should be adopted by public sector organisations. Where appropriate, organisations should use the Framework and other tools, such as Privacy Impact Assessments, to initiate an open dialogue with the public and with stakeholders around new data-sharing initiatives.

Effective co-ordination of the overall strategy

9.19 The current approach to information issues in the public sector is disjointed. In delivering a step change in information management, and breaking through the culture of compliance that views privacy concerns as a threat rather than an opportunity, a strong lead from the centre will be necessary. For this reason, this report recommends that the Lord Chancellor's Department – which already has policy responsibility for data protection matters – take ownership of the strategy and oversee its implementation across the public sector. In specific public sector fields, for instance local government, other organisations such as the Improvement and Development Agency (IDeA) should consider replicating LCD's role, forging strong links to ensure cross-pollination of ideas and best practice.

9.20 The core functions for this co-ordination role are set out in Box 9.3 overleaf.

9.21 As with the Chief Knowledge Officer responsibilities, increasing integration of this co-ordinating role with other information and knowledge functions will be desirable. The co-ordinating bodies will also need to build on experience and expertise elsewhere – such as ONS's work on use of statistics and recording common data items, and building on the Office of the e-Envoy's work on metadata standards and the Ordnance Survey's work on use of Geographical Information Systems.

9.22 The LCD co-ordination function could also assist public sector organisations by increasing their awareness and use of *types* of data that could enhance the services they provide. For example, Geographic Information (GI) can be a powerful tool in tailoring services to individual customers, by

Box 9.3: Co-ordination of the overall strategy – core functions

Policy development and best practice

- Developing the analytical framework.
- Issuing best practice on, for example, data-sharing protocols.
- Monitoring and offering advice on redress mechanisms.
- Updating the strategy as appropriate.
- Developing a consumer focus and acting as the central government point of contact on information issues.

Information sharing and co-ordination

- Information sharing between central government and the wider public sector.
- Making the link between the e-government agenda and privacy issues.
- Horizon-scanning for developments in data use.
- Identifying cross-cutting opportunities for better data use.

Implementation and evaluation

- Monitoring progress with implementation.
- Tracking public attitudes.
- Reporting on progress.

providing the exact location of the nearest school or closest one-stop shop, in being responsive to a complaint about a suspected gas leak or broken street lamp, or policy making focused on particularly needy neighbourhoods or communities.

9.23 Last year, the Intra-governmental Group on Geographic Information conducted a survey to identify barriers to better use of GI systems within the public sector – one of the top barriers listed was the absence of a government-wide information strategy.

As a resource for public sector organisations, in promoting greater awareness and issuing practical guidance, an effective co-ordination function can ensure the maximisation of public sector information assets.

Recommendation 20: To ensure effective co-ordination of the strategy, the Lord Chancellor's Department should take overall responsibility for championing and overseeing implementation of the conclusions of this report – supported by the relevant organisations in specific fields (e.g. IDeA). It should provide a capacity to assist departments and other public sector organisations in modernising their information management strategies, facilitate resolution of inter-departmental issues, and build links with existing initiatives in electronic government and the overall modernisation of public services as described above. This will also enable greater alignment of data-sharing policy with policy on data protection.

Better training for information management professionals

9.24 In many respects, information management is in its infancy in the public sector, where public services have sometimes been slow to realise the opportunities provided by new technologies and the move towards e-business and e-government. Consequently, there are relatively few people with policy or operational experience of the issues. The strategy therefore needs to consider the knowledge and skills required to deliver integrated information management and to identify a range of education and training mechanisms that will address this skills shortage and help establish a cadre of information management professionals within the public sector.

9.25 Already, several training packages are available that could be adapted or extended. For instance, the Public Record Office runs a professional training and education programme via a consortium of universities on information and records management in the public sector. Courses are also provided to enable officials to meet the requirements of the Freedom of Information Act. In addition, a number of organisations – including the Department of Health, the Department for Work and Pensions and Thames Valley Police – already deliver training packages focused on anti-fraud professionals. These packages cover the ethical, legal and technical questions, including requirements under the Data Protection Act.

Recommendation 21: To ensure better training for information management professionals, the Centre for Management and Policy Studies, working with training partners and drawing on best practice standards and guidance from, for example, the Public Record Office, should develop a series of training and education programmes for public sector officials involved in data-sharing and information management.

Funding initiatives to support better use of data

9.26 Various funding streams already support better data management, but these tend to focus on hardware and systems rather than softer management processes or smaller-scale changes. Consequently, the perception in many public sector organisations is that existing incentives to improve performance in information management are weak. This position may be exacerbated as the conclusions in this report are implemented successfully – as information is shared more effectively, it is expected that there will be rising concerns about the administrative costs of supplying information, particularly where the supplier receives none of the benefit, whether in improved efficiency or reduced fraud and error.

9.27 In addition, PSA targets are sometimes too narrow and therefore don't recognise or encourage better data use or management. Clear and compatible PSA targets for the different departments and the availability of cross-cutting funds to finance IT investments for shared objectives have assisted in incentivising and facilitating progress. By taking a broader view across public sector bodies, it should be possible to identify where financial incentives and planning mechanisms might best be used to assist organisations in developing better cross-cutting strategies for information management.

Recommendation 22: Departments should consider how initiatives to support better data use can be mainstreamed within their existing financial plans and those that will be set as part of the 2002 Spending Review, building on e-business action plans as appropriate. In addition, e-business action plans – as part of wider business design – should address the issues of privacy protection and better use of data.

10. THE LEGAL FRAMEWORK

Summary

The legal regulation of data-sharing is based on a number of different elements:

- the administrative powers that public bodies have to collect, hold, share and use personal data;
- the common law, particularly the duty of confidentiality; and
- the statutory regulation set out, in particular, in the Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA).

The analysis for this project suggests that the main problems with the legal framework – in terms of delivering the twin objectives set out in Chapter 5 – are focused more on the powers to share data rather than observance of the requirements of the DPA. That said, there needs to be more awareness of how the existing legal framework operates. And compliance with the statutory regulation clearly requires considerable attention – and effort – and raises particular issues for data-sharing involving existing databases. The main problems to be addressed are therefore:

- there needs to be a greater understanding of the legal framework with respect to public bodies' existing powers to collect, use and share personal data and the interaction of these powers with data protection provisions;
- there are specific problems in terms of lack of powers for statutory and common law bodies to share data – with a particular problem that statutory bodies may not have legal powers to share data even where the individual has given their consent to data-sharing; and

- **the mechanisms for introducing new powers to enable data-sharing need to be considered further.**

This chapter deals with the priorities for action in ensuring that public services are clear about what the law does and does not allow and ensuring that they can actively respond to demand for more joined-up services. The Government should also consult on two proposals for legislative changes:

- **the introduction of a general power to enable public authorities to share personal data with the consent of the individual; and**
- **changes to legislative processes for establishing data-sharing gateways, to allow data-sharing gateways to be introduced through secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny.**

Background

10.01 The complex interplay between the different layers of regulation was described in Chapter 3. Essentially, the framework is based on a number of elements, some well established and others that have evolved rapidly in recent years. The key elements of the legal regulation of data flows are:

- the administrative powers of public bodies to collect, use and share personal data;
- the common law duty of confidentiality;
- the Human Rights Act 1998; and
- the Data Protection Act 1998, which repeals and replaces the 1984 Data Protection Act.

Problems with the current legal framework

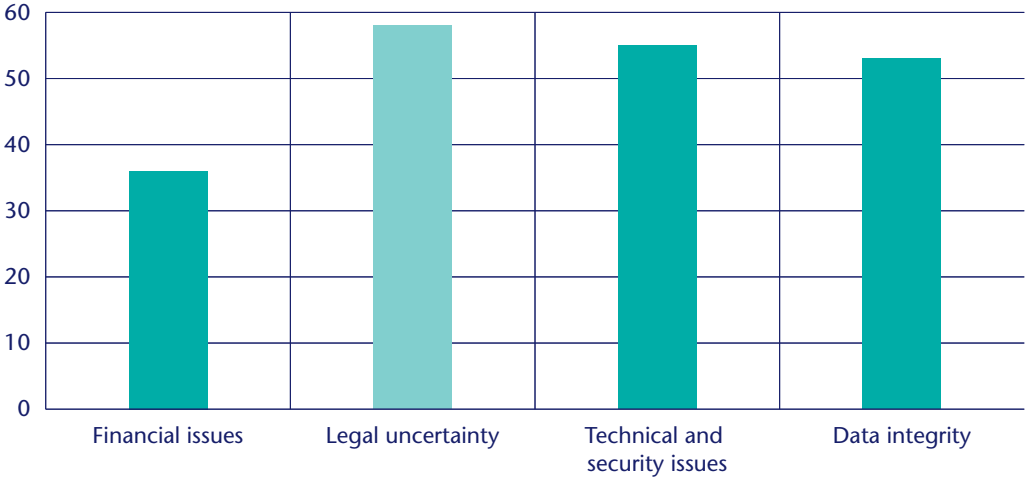
10.02 The legal framework provides a strong level of protection for the individual in the use of their personal information. However, there are three main areas of concern about the overall legal framework, with the first two closely linked:

- there needs to be more awareness of how the current legal framework operates with respect to public bodies' existing powers to collect, use and share personal data and the interaction of these powers with data protection provisions;
- there are concerns about whether existing powers to share data are adequate, given public expectations of improved public services and public bodies' aspirations to achieve a step change in service delivery; and
- there are arguments that existing mechanisms for introducing new powers to enable data-sharing could be improved.

Understanding the legal regulation of data-sharing

10.03 The interaction between legislation and administrative powers has largely been left to individual public bodies to interpret. Consequently, there needs to be greater understanding of what the law actually allows. Anecdotal evidence suggests that the complex nature of regulation prevents the realisation of a number of benefits for consumers through better data use. Indeed, a MORI survey of central government departments showed that legal uncertainty was a major impediment to making better use of data held by organisations.

Fig 10.1: "Which of the following, if any, do you think are barriers to increased data-sharing faced by your department?" – % identifying the specific barrier[83]



10.04 The interplay between the layers of legal regulation is complex, and uncertainty over an organisation's powers to share data is a key factor in inhibiting data-sharing. In more and more instances, innovative public services rely on partnership working between different public bodies, all of whom can have different views as to their ability to share information. This can lead to dissipation of effort and, occasionally, a failure to meet the policy objective.

10.05 Even where a specific statutory gateway is created to enable data-sharing in support of the shared objective, there often remains some uncertainty over what information is covered and how it can be shared. Tools such as data-sharing protocols and codes of practice – which this report advocates further use of – can help to bring some clarity to proceedings, but there can often remain fundamental differences of opinion between organisations.

10.06 Operating the legal framework correctly rests on two related issues – proper interpretation of the DPA and questions of the extent and scope of administrative powers. Each needs to be considered carefully.

Are existing powers to share data adequate?

10.07 Consent may, in certain circumstances and for certain types of bodies, provide a legal basis upon which to share data.

[83] *Attitudes towards Data-sharing: A Survey among Civil Servants.* Survey conducted by MORI on behalf of the PIU, November 2000 to January 2001.

However, local authorities and other statutory bodies may be restricted by the requirement that they can do only what statute allows them to. For statutory bodies, therefore, the consent of the data-subject may not necessarily legitimise the data processing.

10.08 Consequently, several data-sharing initiatives – including many of those cited in Chapter 11 – are currently blocked as the bodies concerned cannot share the information necessary to support the service, even if the individual has consented to the data-sharing. For instance:

- the UK Passport Service (UKPS) would like to issue renewal reminders to passport holders six months before their passport is due to expire. For this scheme to be workable, however, UKPS needs up-to-date address information. The address data held by UKPS is usually out of date, as most people move during the ten-year life span of their passport. UKPS would therefore like to get up-to-date address data from the Driver and Vehicle Licensing Agency (DVLA), but legislation would be needed to enable DVLA to disclose this information to UKPS; and
- local authorities would like to use core Council Tax information – mainly name and address – as the basis for customer management databases in supporting one-stop shops, an innovation that can have major benefits for the community by helping to streamline service delivery. However, the Local Government Finance Act 1992 prevents the use of this data for any purpose other than the administration of Council Tax, regardless of the benefits that could be provided to the community.

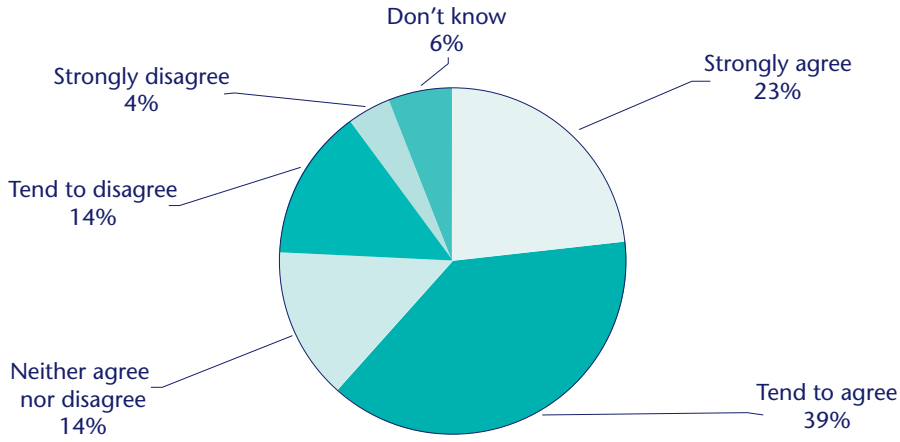
10.09 Of course, consent is not always viable. In many instances data-sharing may need to occur without the individual's consent:

- for operational concerns – the cost of establishing a system based on consent may be too high or the benefits may be realised only if all data subjects opt in;
- for policy objectives – for instance, in tackling crime and fraud or improving enforcement of civil judgments. In addition, effective law enforcement relies heavily on intelligence gathering, where information on the suspect and their known associates may be needed for an investigation; or
- for research, historical or statistical purposes – for instance, the production of anonymised National Statistics. The DPA provides an exemption for secure use in these circumstances.

10.10 The sufficiency of powers to share data in each instance is constantly in question. Where consent is given, organisations may still be unable to share data due to the narrow definition of their administrative powers. In the field of crime, criminals are finding new ways of avoiding detection, and gateways need to be expanded to cope with new threats and new forms of crime.

10.11 Consequently, public bodies are restricted in their options for taking advantage of new opportunities, even where there is explicit demand for new services or where citizens are willing to give consent for their information to be shared. What is clear is that better data use will be a key enabler for more effective public services.

Fig 10.2: "The achievement of my department's key objectives depends on increasing the extent of data-sharing with other government departments."[84]



10.12 But concerns remain that data-sharing powers are insufficient, preventing public bodies from meeting policy objectives and from securing a step change in service delivery. The following box lists – as examples – several areas where data-sharing could provide better services or improve public bodies' ability to tackle crime and fraud, but where the existing powers of the relevant bodies to collect, use and share personal data are insufficient for the proposed purpose. They do not represent established policy, but rather opportunities that will need further examination.

Box 10.1: Current data-sharing opportunities that require further legislation

Better regulation of immigration and asylum – data held by the Immigration Service could potentially be shared with local authorities, the Benefits Agency, Inland Revenue, Customs and Excise and other partners to tackle fraud and illegal working, to support removal activity and to tackle smuggling.[85]

Vehicle Excise Duty (VED) – data-sharing between the Driver and Vehicle Licensing Agency (DVLA) and the Department for Work and Pensions (DWP) to enable disabled motorists to claim VED exemptions more easily.

Protecting children at risk – improving the reliability of List 99 – which lists people banned from working with children and vulnerable adults – and subsequent policing of the register, in order to provide more effective protection for children.

Empty homes – enabling local authorities to share Council Tax data to support the development and implementation of strategies for dealing with empty homes through the Housing Investment Programme.

[84] *Attitudes towards Data-sharing: A Survey among Civil Servants.* Survey conducted by MORI on behalf of the PIU, November 2000 to January 2001.

[85] The report of the Home Affairs Select Committee in January 2001 also noted the importance of data-sharing between agencies in policing Border Controls, and the problems faced in collecting data in the first instance. See www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/163/16303.htm

10.13 The narrow definition of an organisation's purpose or function can also pose problems for sharing information with other bodies or even within an organisation for related purposes. For instance, the Department for Work and Pensions took the view that it needed to obtain data-pooling powers to enable it to share data across the organisation in support of its core functions.

Extending powers to share data – data 'gateways'

10.14 Where it is thought that administrative powers are insufficient, public services have to take powers in primary legislation to establish data-sharing 'gateways'. This can be a long process – and it is important that public services consider the scope within the existing legal framework.

10.15 Sometimes, because of the existing legal framework, public services are often unable to respond to demand as quickly and effectively as citizens demand, even where the public consents to their information being shared between organisations. This inflexibility suggests that there is scope for changes to legislative practices to enable public services to respond to demand quickly and efficiently.

10.16 In requiring gateways to be established in primary legislation, the law can also appear impenetrable to service users. Individual gateways enabling data-sharing between organisations usually constitute one or two clauses in fairly large Acts and the full range of gateways available to an organisation to enable them to share data may be spread through several independent pieces of legislation. Box 10.2 below highlights the case of the Department for Work and Pensions (DWP) where, through no fault of the organisation, different

Box 10.2: DWP data-sharing powers in legislation since 1999[86]

- Social Security Contributions (Transfer of Functions) Act 1999
- Tax Credits Act 1999
- Access to Justice Act 1999
- Welfare Reform and Pensions Act 1999
- Immigration and Asylum Act 1999
- Television Licences (Disclosure of Information) Act 2000
- Local Government Act 2000
- Social Security Fraud Act 2001[87]

[86] Copies of all the Acts listed are available on the HMSO website: www.legislation.hmso.gov.uk/acts.htm

[87] A code of practice is to be issued to ensure that the nature and extent of the information sharing powers – and the penalties for misuse of those powers – are clear to citizens as well as to staff.

information gateways are spread through different Acts.

10.17 There is room to ensure greater internal and external clarity where information gateways are established, how they are established and how, if at all, they are indexed. For citizens, greater clarity over what powers public bodies have to share data would enable them to make more informed choices in their interactions with organisations. For the public bodies themselves, there is the potential that a different process would enable them to respond to data-sharing opportunities, or public demand for new and innovative public services, more effectively.

Tackling the problems

10.18 The ability of public bodies to share information to facilitate service delivery, better policy making or to enable more effective tackling of crime and fraud is inhibited by the three factors listed below:

- uncertainty about whether the powers that organisations have to share data apply to some types of data;
- some concern over whether existing powers are sufficient, particularly in instances where the individual consents to the data-sharing; and
- further concerns over whether existing processes for establishing data-sharing gateways inhibit the delivery of effective public services.

Building greater clarity and confidence in the legal regulation of data-sharing

10.19 The problems are particularly apparent outside central government, particularly where several organisations work in partnership to deliver a service. Organisations tend to adopt a safety-first approach, occasionally hiding behind the existing legal framework as the key barrier to data-sharing. Data-sharing is inhibited as different bodies have different interpretations of their powers, and have recourse to different sources for these powers depending on their status.

10.20 There is a clear need for further guidance for public bodies. In order to ensure as much consistency in approach as possible, general guidance should be issued offering key information – but not replacing the need for a more thorough local appreciation of issues. In instances of real difficulty a central source of guidance and expertise should also assist in brokering a solution.

10.21 The Lord Chancellor's Department (LCD), which now has policy responsibility for data protection, should develop and own this guidance, in partnership with the relevant stakeholders. The guidance would clearly need to be readily available to public services and all relevant organisations.

Recommendation 23: The Lord Chancellor's Department should develop guidance on the interpretation of administrative powers and the key principles within the Data Protection Act with regard to how data-sharing can and should operate within the existing legal framework.

Possible legislative changes

10.22 As public services become increasingly joined up, focusing on the needs of particular client groups – such as children – or particular problems – such as fighting crime – it will be essential to ensure that the legislative framework underpinning data use in the public sector does not lock information into a particular organisational form. In order

to secure the best use of data, it will be necessary to ensure that information is interchangeable between services, enabling service providers to offer truly seamless services.

10.23 The evidence in this report suggests that the current legislative approach to data-sharing is restrictive, and that there may be scope for change in two key areas:

- enabling data-sharing where the individual consents to their personal data being disclosed to a third party; and
- changes to the way in which data-sharing gateways are established in statute. This is particularly important in instances where consent is not viable.

Data-sharing with consent

10.24 Increasingly, there is popular demand for new, innovative and high quality public services. Better data use and high quality information management will be a key enabler if public services are to respond to these challenges. In many cases, public services are able to share information without the need for a specific addition to their administrative powers. Their existing *vires* are sufficient to provide a lawful basis for sharing information. However, there are too many instances where administrative powers are thought to be insufficient, and these instances are likely to increase as public sector bodies use information more imaginatively or seek to be more proactive in their interactions with citizens.

10.25 In such circumstances, public bodies have to seek one-off additions to their powers to share data, through the creation of data-sharing 'gateways' in primary legislation. As noted above, this process can be time-consuming. Given high and rising expectations of public services and the consequent need to ensure public services can improve their ability to use data more effectively to improve service delivery, there is perhaps an argument for enabling gateways to be established more quickly than is presently the case. A potential model for achieving this would be to enable gateways to be established via secondary legislation.

10.26 Enabling legislation needs to consider data-sharing on two levels:

- where the data subject consents to their data being shared; and
- circumstances where consent is not a viable option.

10.27 In the former case, a single gateway could be envisaged that would enable data-sharing with the individual's consent. Given the individual level of control inherent in this system and the regulation afforded through the DPA and HRA, further codified safeguards – excluding the non-statutory safeguards discussed in this report – might not be necessary, so long as the individual was able to change their mind at any time.

Recommendation 24: The Government should consult on the introduction of legislation to enable public bodies to share personal data with the consent of the data subject. This power would need to operate without prejudice to existing data-sharing gateways and practices.

Data-sharing without consent

10.28 There are, however, several circumstances in which the individual's consent may not be an appropriate mechanism for enabling data-sharing. In particular, in fighting crime and fraud, in improving civil enforcement, tackling

fine-evaders and in providing core services such as health and welfare, operational necessities will often militate against obtaining the individual's consent. In these circumstances, a different model would be necessary.

10.29 The move to establishing such data-sharing gateways through secondary legislation would be a substantial step, one which would necessitate clear, codified safeguards to be attached to the enabling legislation. For instance, any or all of the following safeguards could be attached to any possible model:

- the need to ensure effective Parliamentary scrutiny, together with consultation with key stakeholders, such as data subjects and the Information Commissioner;
- requiring secondary legislation to be passed under the affirmative resolution procedure and/or making each order subject to a sunset clause, requiring orders to be renegotiated after a set period;
- specifying which public bodies were covered by enabling legislation, or the types of personal data that could be shared through gateways created under the enabling legislation; or
- requiring public services to set in place adequate safeguards. A Code of Practice, which included standard internal sanctions for abuse, could even be included as one of the requirements within the legislation.

10.30 The move to secondary legislation would, with these safeguards, be a balanced package. The move to secondary legislation is indeed a substantial step, but it should be borne in mind that the courts would have the right to strike down secondary legislation that contravened the Human Rights Act. The onus would therefore be on departments to illustrate proportionality.

Recommendation 25: The Government should consult on change to enable data-sharing gateways to be established via secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny.

10.31 Clearly, enabling legislation would be a significant step. There is a careful balance that needs to be struck between enabling public services to establish modern methods of service delivery for the public good, and the need to ensure that Parliament has adequate opportunity to examine such data-sharing proposals in detail.

10.32 There are several possible models for change, and the model presented above is one of many that could be envisaged. Possible changes to legislative processes should not be seen in isolation. The recommendations set out in this report should be viewed as a coherent package, designed to enable e-government and a step change in service delivery with public trust and engagement.

10.33 The Government would welcome responses to the proposals listed in Recommendations 24 and 25 above. Responses should be sent in by 12 July 2002 to:

Paul Henery
Freedom of Information & Data Protection Division
Lord Chancellor's Department
Room 912
50 Queen Anne's Gate
LONDON SW1H 9AT

Fax: 020 7273 2684

E-mail: foiu@homeoffice.gsi.gov.uk

11. SERVICE-SPECIFIC PROPOSALS

Summary

The project has identified a number of specific areas where public services should look to make progress in using personal information more effectively in delivering services; in giving the public more control over their own data; and in using data more intelligently to improve efficiency.

These are set out in more detail in this chapter.

Progress in a number of these areas may be dependent on departments securing statutory backing and resources in the usual way.

11.01 There are 19 proposals for action in specific areas, grouped under four broad headings:

- more joined-up and responsive services;
- more effective and better targeted policy making;
- tackling crime and fraud; and
- tackling debt.

Some of the proposals listed are already Government policy; others will need to be examined in greater detail before final decisions are made. In addition, many of the proposals cited may require legislative change to enable data-sharing.

More joined-up and responsive services

Identifying and supporting children at risk of social exclusion

Objective: To ensure early identification of children, young people and their families at risk of social exclusion and ensure they receive the support they need.

Need for better data use: Information-sharing across agencies to build up a holistic view of children's needs, and ensure children do not slip through the net.

Issues: Support for children, young people and their families at risk of social exclusion. Local agencies need to be able to identify quickly children at risk of social exclusion and provide the support they need to keep them on track. At present, children can fall through

the gaps in service provision if services fail to identify them early enough. Lack of information-sharing can hinder the development of a holistic joined-up response to the problems faced by children.

The Children's Fund has been established as a new part of the Government's strategy to tackle child poverty and social exclusion. The Fund will support services to identify children and young people between the ages of 5–13 who are showing early signs of difficulty, and provide them and their families with the support they need to overcome barriers and disadvantage and start achieving their potential. Its aim is to reduce truancy and exclusions, improve educational performance and reduce youth crime and reconvictions.

In order for the Fund to add value to existing services, the range of preventative services already being provided will need to be mapped. By linking this to the analysis of risk factors and interpretation of need, gaps can be identified. Information-sharing across agencies is therefore vital, particularly among local education authorities, social services and the police. Common information-sharing practices will be necessary. New partnerships should be able to draw on practices already developed and tested in local government. These issues are also being explored as part of the current Spending Review.

Issuing photocard driving licences

Objective: To enable more efficient issue of photocard driving licences.

Need for better data use: Further links between the Driver and Vehicle Licensing Agency (DVLA), and the United Kingdom Passport Service (UKPS) would enable applicants to supply their UK passport number rather than send original documents to DVLA to support their application for a photocard licence.

Issues: DVLA and UKPS have a long-standing agreement to exchange information to assist efficiency and customer service in the issuing of photocard driving licences. Authentication of identity is required on the issue to a driver of the first photocard-style licence. DVLA now issues only photocard licences and a passport supports 60 per cent of applications. Data-sharing links with UKPS would allow applicants to supply their UK passport number to allow the details to be confirmed without the need for sight of the original document. This would remove the burden from the applicant of parting with their passport and reduce DVLA's costs in handling and returning these documents, while maintaining rigorous security standards.

The proposal is hampered by the lack of legislation to support the necessary data-sharing gateway, but advice from the Information Commissioner's Office suggests that the scheme could go ahead – on a temporary basis – with the consent of the data subject. It is hoped that a pilot scheme will be implemented some time in 2002, subject to IT capability having been established.

Better access to health records

Objective: To put in place the essential infrastructure to enable services to be delivered electronically and improve the quality of patient care.

Need for better use of data: For healthcare professionals to have electronic access to an individual's medical history and current condition to enable them to provide the highest quality care.

Issues: The NHS Plan sets out proposals for radical modernisation in services, requiring investment in the information management and technology (IM&T) infrastructures to deliver integrated services across all NHS

organisations and with local authorities with social services responsibilities. Existing Local Information Strategies and Local Implementation Plans need to ensure their local strategies develop and implement plans to support Information for Health and Information for Social Care. Organisations will need to ensure that there are coherent actions both at a national and local level to ensure compatibility for delivering integrated electronic records and national applications adhering to the e-GIF standards and policies. A number of key issues are being addressed:

- use of the NHS number in local authorities;
- an integrated communications infrastructure for all those involved in the provision of health and social care services;
- agreed technical and clinical standards for the development of electronic records; and
- development of field-based IM&T solutions to support the implementation of the NHS Plan.

The Information Policy Unit is developing a strategic outline case for broader national infrastructure services to develop closer working relationships with local authorities and other partners. There are sixteen demonstrator projects looking at developing reproducible solutions in areas such as closer working across health care sectors.

Services for those in real need

Objective: To streamline legal aid applications and reduce fraud.

Need for better data use: Case-by-case linking of Department for Work and Pensions (DWP) files to legal aid applications to speed up the application process and to secure the system against fraud.

Issues: Legal aid eligibility is currently means-tested, and many eligible customers are benefit claimants. At present, they have to go through the full means test, which involves discussion of personal details at what can be a very difficult time for clients. Although it is not a major problem, the legal aid system has also been open to fraud, with ineligible clients able to claim legal aid.

Better data-sharing between DWP and the Legal Services Commission (LSC), which administers the legal aid scheme, would eliminate duplication of effort and provide better security against fraud. Enabling the LSC to use DWP data, where benefit claimants applying for legal aid have already gone through a means-test process, would lessen the sense of intrusion at what can be a difficult time for litigants. In addition, data-sharing between DWP and the LSC would provide more effective safeguards against fraud and error, releasing resources to ensure that they are targeted where they are needed.

Ex-offenders

Objective: To reduce reoffending.

Need for better data use: Information-sharing between local agencies to ensure joined-up support for offenders on release and aid their assimilation into their communities.

Issues: On leaving prison, many offenders do not have access to the services and support they require to help them resettle effectively into society. Many offenders leave prison with poor levels of educational attainment, poor employment prospects and with special needs – for instance, mental health problems. In addition, they may not have housing arranged and may have to wait some time before being able to receive benefits. Consequently, the likelihood of their reoffending increases.

A large part of the problem is that services are not joined up, and do not share information to help them provide a targeted support service for each offender. Better use and exchange of information by a range of services – including probation, welfare, social services, education, housing and others – would provide a more joined-up response to individual needs. In order to avoid stigmatising service users, this help could be time-limited to, for example, two years, or until such time as it is judged that the offender is firmly established in their community and thus less likely to reoffend.

The Social Exclusion Unit is looking at how government departments might work together more effectively to reduce reoffending by ex-prisoners. It is already clear that better data-sharing between agencies will be a key feature.

Modernising civil registration

Objective: To enable on-line registration of births, marriages and deaths and electronic access to registration records.

Need for better data use: Moving local paper-based files onto a central IT platform to enable modernisation of the registration service.

Issues: The civil registration system in England and Wales plays a vital role in securing and protecting basic human rights by providing individuals with a name and status within society, a facility for marriage, evidence of parentage and evidence of entitlement to inheritance and insurance. The system is mainly paper-based, making requests for information time-consuming, inflexible and not based around customer needs, while also being open to fraud.

The White Paper *Civil Registration: Vital Change* published on 22 January 2002 proposes changes to the law to enable modernisation of the system, including on-line registration. A modernised system will continue to secure individuals' basic rights but be much more flexible. It will allow citizens to register births and deaths in a variety of ways, including by telephone or the Internet. To work properly, birth information will have to be notified electronically by health authorities, and in time, following consideration of the issues arising from the Shipman Inquiry, there could be electronic links between doctors, coroners and registrars to share information on deaths. The development of a single administrative register for NHS patients could also provide opportunities for sharing data.

A modernised system should also allow greater use to be made of civil registration data – public services could use the electronic registers to reduce their dependency on paper documents. For instance, information on deaths could be provided automatically to DWP and its agencies so that pensions and other benefits do not continue to be paid to the deceased. Other information may be provided with the consent of individuals for verification purposes, for instance to the UKPS or the DVLA. The use of the Government's Authentication Framework should assist citizens accessing the data.

Improving services for families (i)

Objective: To ensure families are aware of, and able to access, the full range of services available to them.

Need for better data use: To enable NHS, education and social care agencies to share information with Sure Start partnerships in

order to tailor services to family needs and effectively monitor the impact of the services.

Issues: Sure Start aims to ensure that families with young children receive the services that are right for them by better understanding each family's social and medical situation. Services are delivered by a wide range of service providers – national, local, public, private and charitable, each of which holds its own records and has its own rules, systems and practices for records management and data-sharing. The legal permissions for data-sharing are restrictive or unclear – the recommended practice for Sure Start partners is to collect and share information with the consent of the family. However, Sure Start programmes face difficulties in obtaining this consent as often they do not have access to lists that show where all the children under 4 in the Sure Start areas live.

Since Sure Start partnerships are based on geographical communities, they do not necessarily coincide with organisational boundaries. The result is that it is proving very difficult for Sure Start partnerships to collate the necessary range of information. Some partnerships have dealt successfully with these difficulties by agreeing among the partners a data-sharing protocol which spells out key common practices – how data will be stored, updated, secured – and allocates responsibilities. Sharing this experience will give an important boost to the new partnerships still establishing themselves. The Sure Start Unit aims to share examples of good practice in guidance that will be available nationally.

The Department of Health and the Sure Start Unit will consider whether legislation is necessary and desirable to enable basic personal information on name, address and date of birth of children under 4 to be shared between NHS agencies and Sure Start partnerships.

Improving services for families (ii)

Objective: To ensure families are aware of the full range of services available to them.

Need for better data use: Greater use of the Child Benefit (ChB) database to inform families and parents of the services available to them.

Issues: Services for families are increasingly delivered locally, by a range of partnerships and service providers. Some families are unaware of the services that are available, or of the services they might be eligible for. Government has a duty to ensure that everyone eligible for services is fully aware of their options, enabling them to make choices about which services to take advantage of.

Using the ChB database would enable government to send targeted information to parents, drawing their attention to the services offered in their region, and giving contact details for further information. In this way, the ChB database could be better exploited to ensure that families with young children are aware of the full range of services available to them, nationally and in their community.

Streamlining services for motorists

Objective: To make it easier for motorists to tax their vehicles and keep their records up to date.

Need for better use of data: Enabling data-sharing within the Department for Transport, Local Government and the Regions (DTLR) and between DTLR and the insurance industry would enable the development of

modern electronic services for motorists that would allow people to tax their cars without the need for producing paperwork each time.

Issues: DTLR's Driver, Vehicle and Operator (DVO) group is working to restructure its service-delivery processes around customer needs. To achieve this aim the group needs to share data that is currently held for single purposes. This need not only covers data held by the group, but also that held by other government departments and the motor insurance industry. If the DVO group could improve its use of this data to provide more effective, joined-up services to the end-user, there would be a number of benefits. For instance, by linking together information on drivers and their vehicles, the public could have access to a one-stop shop Internet and call centre service for relicensing their vehicles and for registering changes of details, ownership and address. Enabling this would improve voluntary compliance and allow the effective targeting of those who attempt to evade paying their dues, but is frustrated by the current rules on data-holding and data-sharing.

Improving information on the property market

Objective: To simplify the collection of data on sale and purchase of land and property and to improve transparency in the property market through enhancing access to this data.

Need for better data use: Government already collects information on property transactions, including price paid, through the Land Registry – this information is in the public domain. Separately, the Valuation Office collects data on land transactions, including price paid, both for residential and non-residential purposes. They also collect data on the physical characteristics of land and buildings and on lease terms and rents in order to assess rateable value. A third agency, the Stamp Office, requires property owners to provide information on the transaction price in most property transactions in order to levy stamp duty. The three agencies are currently restricted in the amount of information they exchange and share.

Issues: There are three key issues:

- there may be opportunities to rationalise the collection of data;
- there is a need to review the level of confidentiality applied by the different agencies to each item of data. The recent decision by the Lord Chancellor to bring Land Registry price paid data into the public domain calls into question the appropriateness of a 'closed' regime maintained by others. In particular, a more transparent basis for business leases, which in turn form the basis for rating assessments, could reduce the level of appeals. Taking this one step further, as part of its modernisation of the rating system, the Valuation Office Agency (VOA) could publish details of its valuations for rating – i.e. the build-up of the rateable values that are currently contained in rating lists – to improve transparency and understanding by ratepayers. A move to greater openness could also help to bring transparency to the property market; and
- the opportunity to bring together aggregate statistics on the physical stock of land and buildings and their current value would be a powerful tool in developing policies for the future of the built environment. This use could proceed independently of decisions on confidentiality.

Movement in each of these areas will improve the availability of information on

local and national property markets, with clear benefits for homeowners and buyers, particularly first-time buyers. Better understanding of the nature of markets will also help to improve policy-making. The HM Land Registry Quinquennial Review has also highlighted a number of specific areas where action could lead to more comprehensive and transparent information on property and land prices.

More effective and better targeted policy making

Helping children in need

Objective: To reduce the number of children missing substantial periods of school and ensure children do not miss out on core public services.

Need for better data use: Information-sharing between local agencies to advise local education authorities of the whereabouts of children for whom they have a duty to provide education, and to develop an overview of individual needs to enable a more targeted response.

Issues: Every year a substantial number of children are lost from the school rolls and become 'invisible' to the local education authorities which have responsibility for providing their education. However, the majority of these children will be known to other local agencies – GPs, social services, housing authorities, the Benefits Agency, voluntary sector organisations, immigration authorities and others.

At local level, protocols often do not exist for agencies to share information, and where channels of communication are in place data protection issues can be a barrier to providing effective interventions for children. Good practice on joint working does exist in many areas but it is not replicated throughout the country. There is no co-ordinated approach to the spread of good practice.

Better use of the full range of information held by government on this key customer group would enable all services to be tailored to meet their specific needs, ensuring that children are able to make the most of their potential. Information from all key service providers – education, health, social services and so on – would need to be brought together securely in order to enable services to target responses.

Better use of statistical and management information

Objective: To achieve a better understanding of the anti-drugs strategy and how it is working.

Need for better data use: Disclosure of anonymised health information to enable better tracking and evaluation of treatment programmes and better targeting of resources.

Issues: Drug Action Teams (DATs) provide treatment services for drug addicts in the community, whether referred by the courts or self-referred. However, DATs are finding it hard to gain access to even anonymised data to help them evaluate the success of programmes and identify where additional resources are needed to meet demand. Centrally, government needs this information to assess demand on the national scale in order to allocate resources and to evaluate the success of new initiatives. DATs, and other similar organisations, need access to such information to help them develop local strategies.

A large part of the problem is the reluctance of health professionals to share any

information, even where the data are effectively anonymised or pseudonymised and therefore cannot be traced back to a specific individual. Better use of anonymised health data would enable DATs to evaluate effectively the success of treatment programmes and initiatives, and would enable them to highlight areas where further resources would be needed to clear backlogs or to target help at specific populations. At a national level, this information would also enable the Anti-Drugs Co-ordination Unit to better monitor the success of the anti-drugs strategy, and to highlight more effectively areas for further action.

Getting the best from private providers of education and training

Objective: To enable evaluation of 'life-long' education and training – especially where these are supplied by external providers – which could feed into performance-related payments.

Need for better data use: Linking anonymised income information from the Inland Revenue to education and training records to enable better tracking of the post-training performance of individual learners, and better evaluation of training outcomes.

Issues: The Department for Education and Skills (DfES) has commissioned a consultation on proposed new ways of working between the Department and its providers of services to the public (excluding schools and higher education services). New ways of working include an aim to improve the focus on actual outcomes by, amongst other things, modernising the approach to funding and contracting.

One strand of the new proposals is to approve private providers on the basis of their past performance, not only in contractual matters, but in training and education outcomes. We suggest that by tracking the subsequent performance of trainees (e.g. via earnings measured through anonymised tax data from the Inland Revenue) real sustained training outcomes could be detected. This would represent a desired type of innovation in contract arrangements to actively promote, recognise and reward innovative best practice in the design, development and delivery of programmes. The DfES has agreed to consider this suggestion alongside other responses to its consultation document.

Improving urban planning and investment

Objective: To understand and monitor the implications of planning and investment in our towns and cities.

Need for better data use: Disclosure of (anonymised) floor space data in particular and, more generally, information on the location, size and types of commercial and industrial properties, and the changes occurring within the property market.

Issues: The Government response to the Parliamentary Select Committee report on *Shopping Centres and their Future* recommended the development of "a nationally consistent system of retail data collection to be published at regular intervals", which "should reduce significantly the costs being incurred in Public Inquiries and impact studies".

The VOA collects floor space information to arrive at figures for the rateable value of such properties. Some work has been carried out by DTLR to use the VOA data, but much additional work has been needed to make the data useable. There is considerable scope to use the VOA data more widely and at a

more detailed level, but this requires both development of the database and clarification of the legal and policy position on confidentiality, which currently prevents wider exploitation of the information across departmental boundaries.

In particular, a national consistent system of statistics on town and shopping centres should allow local authorities to effectively monitor their town centres, and provide planning inquiries with the information so essential for making informed judgements on the impact of new development proposals. Many local authorities have had to resort to ad hoc surveys of their own to collect data, or have resorted to expensive and often inadequate commercially available data products. Improvements will translate into better planning of urban redevelopment, and into analysis of demand hotspots and local priorities.

Tackling crime and fraud

Better authentication

Objective: To strengthen and streamline the business processes of the UK Passport Service (UKPS) and the Criminal Records Bureau (CRB).

Need for better data use: Better access to other government and private sector databases in order to enhance identity authentication, prevent and detect identity fraud, improve customer service and facilitate electronic transactions.

Issues: Both UKPS and CRB need to confirm the identity of their applicants. Access to data held on government and private sector databases will permit corroboration of an individual's identity history in a far more robust and cost-effective way than the present limited access permits. Greater access to information held in the DVLA drivers' database, the DWP's Departmental Central Index, records held by the Immigration and Nationality Directorate (IND), the modernised civil registration database and, for CRB, the UKPS database will deliver results more quickly to the customer, provide greater assurance of accuracy, reduce errors and uncover and reduce fraud more effectively.

It is important that identity authentication is carried out effectively. For CRB applicants, inaccurate identification could have disastrous results, while a fraudulently obtained passport facilitates fraud on a much wider scale across government and the private sector. At present, the CRB has arranged protocol agreements with DWP and UKPS, and is negotiating a similar arrangement with DVLA. Specifically, the agreements allow CRB to compare applicant data electronically with DWP and UKPS records in order to check consistency. This cross-matching may only be done with freely given informed consent and there are limitations in data access. The UKPS is seeking to reach similar protocol arrangements with DVLA, DWP and IND.

Tackling vehicle crime

Objective: To give the police better information to enable them to tackle vehicle crime and to make roads safer.

Need for better data use: Making more information available to police at the roadside will enable them to make checks against DVLA's drivers' records, the Motor Insurance Database of insured drivers and computerised MOT records.

Issues: Making more information available to the police at the roadside will enable better enforcement. The Criminal Justice and Court Services Act 2000 and the Motor Vehicles

(Access to Driver Licensing Records) Regulations 2001 provide for bulk access to DVLA drivers' records. The latter specifies the lawful access of data by police constables for road traffic enforcement purposes. The Vehicles (Crime) Act 2001 gives police bulk access to the Motor Insurance Database for use to proactively identify uninsured drivers. Forces now need to work towards implementation, enabling officers at the roadside to have access to all the information needed to enforce the law and make roads safer. The Motor Insurance Database has been available to forces on a case-by-case basis since July 2001. Delivery of bulk access is expected in April 2003; drivers' records will be available from January 2002; and computerised MOT records will become available in stages over the period January to July 2003.

Tackling debt

Towards effective enforcement (i)

Objective: To make enforcement capable of delivering higher rates of recovery and capable of delivering results more quickly.

Need for better data use: Allowing regulated enforcement agents access to information on the names and addresses of debtors in order for them to make contact with the debtor to initiate enforcement.

Issues: About 60 per cent of enforcement in the county courts is ineffective because the claimant cannot find the necessary information about the debtor to enable him to take the right method of enforcement, or even to send the bailiffs to the right address. The current enforcement system in the civil courts is reliant on information being supplied by the creditor, and then on the compliance of debtors to provide accurate or truthful information.

LCD's review of enforcement proposes allowing a regulated enforcement agent, as an officer of the court, to have a limited ability to access information from designated third parties, such as other government departments, to confirm that the data provided by the creditor on the identity and whereabouts of the debtor is accurate in order for the enforcement agent to make initial contact with the debtor. Access to, and use of, such information would take place within a legal framework and under close supervision, thereby ensuring tight control and accountability of those carrying out the specified functions.

Towards effective enforcement (ii)

Objective: To facilitate targeted enforcement procedures which are fair to both debtors and creditors and capable of delivering higher rates of recovery.

Need for better data use: Expanding the range of information about the debtor that can be sought by a creditor in order to facilitate enforcement through the introduction of a Data Disclosure Order.

Issues: Currently, creditors have full control over the enforcement process and it is up to them to gather any necessary information and decide which method of enforcement will be carried out by the court. The provision of information is almost entirely reliant on the compliance of debtors with existing procedures. If debtors do not provide the information voluntarily, there are mechanisms in place which attempt to force them to do so, such as the oral examination procedure, but the process inevitably takes time, and it can be difficult to establish

whether the information provided by the debtor is accurate or truthful.

LCD's review of enforcement proposes introducing a mechanism for creditors to obtain a Data Disclosure Order in circumstances where debtors have proved wilfully non-compliant with previous court orders. A Data Disclosure Order would enable the courts to initiate a process to apply for information from designated third parties about the address of the defaulter/debtor's employer, whether the defaulter is in receipt of benefits and the address to which those benefits were being sent, and the extent of the debtor's financial assets in bank or building society accounts. This would enable the court to make greater use of attachment of earnings orders, or deductions from benefits, and provide additional information as to addresses for those enforcing warrants.

LCD has already published a Green Paper and will develop these data-sharing proposals further, building on responses received. Proposals will also be developed with the aid of the Analytical Framework.

Enforcement of civil obligations in Scotland

Objective: To facilitate targeted enforcement procedures which are fair to both debtors and creditors and capable of delivering higher rates of debt recovery.

Need for better data use: Expanding the range of information about the debtor which can be sought by a creditor in order to facilitate more effective enforcement of debt recovery.

Issues: The Scottish Executive is currently carrying out a review of the law of enforcement of civil obligations in Scotland and will consult on proposals for reform. Part of this review is about the obligation for the payment of money and covers the problems experienced, by government and private creditors, in the enforcement of debts owed to them. It is clear that creditors' access to the range of information, about debtors' financial circumstances and assets, held by government and others would enable appropriate and effective enforcement mechanisms to be targeted to avoid procedures which are likely to be fruitless. At the same time, it would offer an additional measure of debtor protection by identifying debtors who do not have the means to repay a debt and would prevent them being subject to excessive or oppressive enforcement measures.

12. IMPLEMENTATION

Summary

To realise this report's strategy for better data use and better privacy protection, the conclusions in it need to be acted upon. In this chapter, we set out the timetable for action and present an integrated implementation plan.

12.01 Implementing the strategy set out in this report will require early action in key areas. The strategy will also need to be updated in time as new technologies and new business processes emerge.

12.02 The recommendations listed in this report cover a wide area, with short- and long-term activities. Priority action should take place where benefits for the citizen can be quickly realised:

- development of service-specific **privacy statements**, codes of practice and model protocols. Many examples of codes of practice and model protocols are already available and could be readily adapted to meet local needs. While privacy statements will depend on the final version of the overarching Public Services Trust Charter, public bodies should look to produce early drafts;
- wherever possible, further development and implementation of the **service specific proposals** for better data use set out in Chapter 11;
- plain language **information for citizens** – explanations of citizen rights and information-sharing activities. Service providers routinely update their literature, and this should be an opportunity to develop new leaflets, posters and other materials that can engage citizens more effectively. The Information Commissioner also has an ongoing role in ensuring that the public are aware of their rights;
- improving **mechanisms to ensure data are correct.** Where information is found to be incorrect, or where it has been mishandled, public bodies should ensure that information can be updated quickly and efficiently, reducing the impact on individuals. Service providers should also ensure that the public are aware of complaints procedures, and that complaints are dealt with quickly and efficiently; and
- identifying a **named senior manager** responsible for the handling of personal information. Ensuring that service users know where to direct enquiries, and that there is a clear point of access for information issues.

12.03 Public service providers should also take early action internally to ensure that the strategy set out in this report can be implemented quickly. For instance, through:

- reflecting the strategy in **e-business action plans**, as part of wider business design. The next iterations of e-business action plans should cover this report's conclusions, setting out what actions departments are taking to build public trust, integrate information management functions and improve service delivery and privacy; and
- making use of the **analytical framework** in assessing new data-sharing initiatives.

12.04 At the same time, work in other areas will take some time to come to fruition. In particular, work on service identifiers, smart cards and authentication technologies and any possible changes to legislation will need to take place over a longer timescale, to ensure that final products are high quality and have the potential to realise the benefits envisaged in this report.

Implementation

12.05 Implementation of the conclusions listed in this report will lead to significant advances at the macro and micro level. However, measuring the impact of individual proposals will be difficult, as the linkages between the conclusions are strong – successful delivery of the strategy set out in this report will depend on simultaneous action in several areas. Nevertheless, it is possible to draw out some key success measures, such as:

- increasing public trust in how information is used by public bodies both generically and by specific service providers – the Information Commissioner already runs public attitudes tracking research which could be expanded or adapted to measure trust;
- increasing rates of take-up where citizens have a choice whether to opt in to a service – the measure could focus on the take-up of smart cards or other technologies;
- quality measures and audit results – backed up by independent assessment, perhaps through NAO reports; and
- decreasing error rates, leading to reduced losses through fraud and error.

12.06 The Lord Chancellor's Department will take lead responsibility for implementation of the recommendations set out in this report, working closely with the Cabinet Office and other Departments. Resources for this implementation work will be considered as part of the current Spending Review. The implementation plan set out in the report is dependent on appropriate resources being available. A revised implementation plan will need to be developed at the end of the consultation process, taking account of the responses to consultation on specific proposals and the available resources.

12.07 The success measures listed above are primarily measures of activity. The Lord Chancellor's Department should develop further success measures as an early part of its work programme, examining additional areas such as declining requests for duplicate information and improved use of existing information.

12.08 The Lord Chancellor should report on progress with implementation of the strategy set out in this report 12 months after publication. Public services should also report on progress as part of their annual reporting cycle.

Summary of conclusions

12.09 The table below records the 25 recommendations listed in the report, suggests an appropriate lead organisation to take responsibility for action and outlines a proposed integrated timetable for implementing the strategy and moving towards better data use and improved protection for personal privacy.

	Recommendation	Lead responsibility	Timetable
1.	The Government should consult on the Public Services Trust Charter, a draft of which is published here. The Charter sets out the guiding principles and key commitments made to the citizen in protecting their privacy and personal data in their interactions with public services. All public sector organisations should look to embody these principles in service-level privacy statements *describing precisely in each case* how personal information will be shared in support of service delivery or research and evaluation, and how individuals can get access to their personal data. In turn, these privacy statements will be key instruments by which the public is informed and in helping to secure consent where information is shared to support delivery of public services. They must therefore be easily and readily available to the public, where appropriate at physical outlets and websites. To ensure implementation of these privacy principles and undertakings, each service-level privacy statement will need to be embodied in working-level codes of practice and information sharing protocols, themselves underpinned by management guidance. These should also be made publicly available.	The Lord Chancellor's Department (LCD) should lead consultation on and subsequent development and adoption of the Public Services Trust Charter. Service-specific statements will be the ultimate responsibility of individual public bodies, building on the LCD's work and identified best practice. Lower-level documentation – codes of practice, management guidance and data-sharing protocols – is for individual service providers to resolve, building on established good practice.	The Trust Charter is published here for consultation. The Government would welcome responses by 12 July 2002. The Trust Charter should be finalised by autumn 2002. Guidance underpinning the Charter should also integrate the Public Record Office's (PRO) activities, as well as data protection requirements. Service-specific statements will be dependent on the overarching Trust Charter, but early iterations should be in place by summer 2003. Good examples of many of these materials are already available, and should be updated – or developed where they are not present – as soon as possible.
2.	In order to provide better information to the public on information held by public services, those public bodies covered by the Freedom of Information Act should consider publishing a statement on sets of data held and information sharing practices as part of the publication schemes which public sector bodies are required to publish under the Act.	Publication schemes are the responsibility of individual service providers, although much of the information will already appear in Information Asset Registers and, as such, could be replicated easily.	Ongoing. In line with existing plans for implementation of the Freedom of Information Act, public services should look to work collaboratively with the Information Commissioner on publication schemes, building on the proposed methodology and subsequent work.
3.	Public service providers should consider ways to improve the public's access to their personal data. As part of this, they should also consider setting clear targets for performance, which should ensure steady improvements against the statutory target for response to information requests, and monitoring performance against these targets.	Subject access – and less formal access – procedures are the responsibility of individual service providers.	Ongoing. The problems posed by legacy IT systems and paper files are great, but future system design and other improvements could lead to significant gains.
4.	Public sector organisations should develop clear explanations of the public's right to access personal data and of access request procedures. This should include a clear point of contact. The information should be provided to customers at point of service, whether on websites or in other publications.	Information on specific services will be for the relevant public body to produce, but the LCD should also develop model publications and build up a 'library' of good practice.	Ongoing. Literature is constantly being updated and reviewed, so new publications could be updated to take account of emerging issues and changes in technology and processes.

	Recommendation	Lead responsibility	Timetable
5.	Public sector bodies should examine existing procedures to enable the public to correct their personal information to identify whether procedures can be simplified and improved. They should also consider setting targets for response, and monitoring and publishing performance data.	Procedures are the responsibility of individual public bodies, but the LCD should also look to monitor performance and share best practice.	Ongoing. Public bodies should look to examine existing procedures, with a view to identifying improvements.
6.	The public should have access to quick and efficient procedures for dealing with complaints about the handling of personal information. Public service providers should therefore consider improvements to existing complaints procedures and new mechanisms for dealing with complaints, including an examination of the potential for adopting Alternative Dispute Resolution procedures.	Internal complaints procedures are the responsibility of individual public bodies, although the LCD will need to share best practice.	Ongoing. Service providers should look to examine existing procedures, with a view to identifying improvements.
7.	All public sector organisations should have a named senior manager with clear responsibility for the handling of personal information. They should also have a clear first point of contact for members of the public on personal data issues. Internal measures to identify and sanction staff for misuse of personal data should be reviewed.	Identifying and publicising these roles will be the responsibility of individual organisations. Once identified, senior managers should work with personnel units to review internal sanctions for misuse of data.	Organisations should have these responsibilities allocated and publicised by Autumn 2002. Some bodies will already have local arrangements in place, such as the Caldicott Guardians, which should continue as appropriate. An early task for senior managers should be a review of internal measures.
8.	The Information Commissioner should continue and expand current activities to promote public understanding and awareness of their rights and obligations. Public services should also promote greater understanding through plain language explanations of DPA and FoI.	The Information Commissioner has a separate, ongoing role to ensure the public are aware of legal provisions and their rights. Publications are produced by individual organisations, although from time to time central guidance may be issued.	Ongoing. In line with existing plans for implementation of the Freedom of Information Act, service providers should look to include information on rights and access procedures in all relevant publications.
9.	To improve the accuracy of data, and reduce the potential for mistakes or inappropriate use when data is shared, public services should consider introducing standards for recording common items of data and for labelling data sets (in terms of their purpose, scope and limitations). A simple quality field in which key quality measures are recorded should be included, where appropriate. As part of this, the Office of the e-Envoy should continue to give high priority to progressing the development and implementation of the Data Standards Catalogue of standardised data fields, giving emphasis in the work to those most commonly used and of most value to data-sharing, such as name and address. This should draw upon the data quality work done by ONS. The Office of the e-Envoy should also continue to give high priority to driving forward the implementation of its recently published metadata standards.	The Office of the e-Envoy is leading work on standards and metadata. ONS and PRO have also completed important work in this area, and it will be important for public services to draw on their expertise.	The OeE has already published much of this material, and has developed an implementation strategy. Public bodies should implement the strategy, working in partnership with the OeE.

	Recommendation	Lead responsibility	Timetable
10.	To encourage widespread adoption of such standards, the Lord Chancellor's Department, working in conjunction with the Public Record Office, should facilitate the development and dissemination of model data-sharing protocols and codes of practice as a resource to public sector organisations. This work will need to draw on a wider understanding of the overall information architecture of government, which maps the creation, flows and uses of information sets, establishes criteria for its sharing, retention and disposal, and allocates responsibilities for sustaining access, quality, reliability and safe-keeping.	The Lord Chancellor's Department will take the strategic lead for this work, working in conjunction with the Public Record Office (PRO) and ensuring that the results can be accessed easily by all public bodies.	The LCD and the PRO should immediately begin identifying and collating examples of best practice, building up a library of material. Model protocols should be finalised by spring 2003 – this allows for consultation with key stakeholders, including the Information Commissioner.
11.	Methods for measuring data accuracy and reliability for privacy and data-sharing purposes should be developed to enable public sector organisations to assess their performance and benchmark against others. The Lord Chancellor's Department should draw on and integrate the work already being done in ONS, the National Audit Office (NAO) and the Information Commissioner's Office to develop a body of knowledge and a set of agreed methodologies for measuring and improving data quality.	The ONS will need to lead this work, building on the expertise of and work already completed by the NAO and the Information Commissioner.	This methodology should be ready by the end of 2002, and the Lord Chancellor's Department will need to work collaboratively with organisations to facilitate implementation.
12.	Internal and external audits should be used across the public sector to improve data accuracy and reliability. Using the Information Commissioner's data protection audit manual as a starting point, the Lord Chancellor's Department should draw together the strands of work in the public sector to develop a data quality audit methodology. When developing new data-sharing proposals, public services should consider using the audit methodology as a diagnostic tool in order to assess the quality of the data in question. Public service providers should also consider whether the results of data quality audits, as part of an overall assessment of fitness for purpose, should be included in any consultation on new data-sharing proposals. As progress is made in implementing the strategy outlined in this report, public audit bodies should also consider giving more attention to information management issues in the public sector, adopting an agreed audit methodology for information management studies they undertake, and publishing data quality measures.	The LCD, working in partnership with the ONS and the PRO, should lead work on developing an audit methodology, building in legal admissibility requirements as necessary. Individual organisations will need to consider including audit outcomes in consultation on a case-by-case basis. Public audit bodies will need to consider how they approach information management issues in their work.	Building on the work already completed, the LCD should look to issue the methodology by the end of 2002; this will also need to be reviewed and updated thereafter. Public services should consider assessment in principle and subsequently case by case once an agreed methodology is available. Public audit bodies should consider including information management issues in their next work programme.
13.	The public sector should at least match best practice in the private sector for information security. As part of this, the ISO17799 standard and its associated processes should be adopted across the public sector to provide privacy safeguards. The Office of the e-Envoy and the Communications-Electronic Security Group should continue actively to monitor the development of new technologies and safeguards which could enhance the protection of personal data, building on the existing Security Framework and the e-Government Interoperability Framework.	Central government is already committed to achieving ISO17799 accreditation. The wider public sector should also consider adopting this standard. The Office of the e-Envoy and the Communications Electronic Security Group should continue to monitor developments in this field.	The wider public sector should consider aligning adoption of security standards in existing e-government commitments. The OeE and the CESG should also consider publishing a review of available/ emerging technologies and begin to assemble a 'library' of information – references to useful tools and knowledge, best practice, what's worked, etc. – for use by public sector organisations.

	Recommendation	Lead responsibility	Timetable
14.	Public sector organisations should require information and records management systems to support best practice in ensuring internal security against possible misuse of personal data, and in managing and controlling access to that data. They should ensure that personal data are held in systems which follow best practice in managing access to information held in the system, and in providing audit trails which record information about who has accessed, or carried out operations on, the data. These principles should be applied to new system design.	The design, development and implementation of new systems will be for contracting organisations to consider. However, there is also a role for the Public Record Office, the Office of the e-Envoy and the Office of Government Commerce in developing best practice and guidance for procuring agencies.	Ongoing. Organisations should look to build privacy protection, safeguards and audit trails into new system design. The OeE should encourage organisations to include audit trails and privacy enhancing technologies in their e-business plans. The OGC should also include these requirements in guidance on developing user requirements and on procurement.
15.	The Government should give further consideration to the broader issues of identification and entitlement to services in the round.	The Home Office should lead this review, in partnership with the Cabinet Office and other interested stakeholders.	The review should look to begin immediately, and to present options for change as soon as possible.
16.	Government should develop a programme of smart card demonstration pilots in specific service areas, in line with the Framework being developed by the Office of the e-Envoy – including consideration of the importance of giving cardholders access to the data held on the card. The Office of the e-Envoy should work with service providers to ensure that a sufficiently broad range of markets and functions are tested and to ensure that interoperability is a key component of system design. This will increasingly allow citizens to make their own choices on what information – covering both the public and private sectors – they carry on their smart cards.	The OeE, working with public sector organisations.	The OeE should bid for funding to scope possible projects in the normal way. Funding for pilots should then be considered in due course.
17.	Authentication technologies have the potential to enable public services to provide high levels of security for personal information and to ensure accurate electronic identification and authentication – which in turn will facilitate the realisation of consumer benefits in public services. Given the relatively slow pace of private and public sector development of these tools, the e-Envoy should assess the costs and benefits of increased government involvement in the development of authentication technologies. Potentially, a series of significant public sector pilots – for instance, giving civil servants a smart card or similar device that could be used to create digital signatures at work and which could be taken home for the same purpose in their life outside work – could encourage swifter development of consumer tools. These pilots could test the functionality and infrastructure necessary, and encourage interoperability with the private sector.	The Office of the e-Envoy.	The OeE should bid for funding to scope possible projects in the normal way. Funding for pilots should be bid for in due course.
18.	Public service bodies should consider integrating the functions set out in Box 9.2 on page 93, including through an evaluation of the appointment of a board level Chief Knowledge Officer as a means to ensure integration of information issues into decision-making processes. Ideally, Chief Knowledge Officers would be responsible for integrating, over time, the disparate functions of legislative compliance and business planning.	Individual organisations will need to review existing information management structures in order to assess their own need for integration.	The Lord Chancellor's Department should look to review their position immediately. Public bodies should carry out an initial assessment by the end of 2002. Subsequent assessments, if needed, should take place as necessary.
19.	To promote more consistent decision making across public services on privacy and data-sharing issues, the Privacy and Data Use Analytical Framework should be adopted by public sector organisations. Where appropriate, organisations should use the Framework and other tools, such as Privacy Impact Assessments, to initiate an open dialogue with the public and with stakeholders around new data-sharing initiatives.	The Lord Chancellor's Department should facilitate implementation of the Framework.	A final version of the Framework should be agreed by autumn 2002.

	Recommendation	Lead responsibility	Timetable
20.	To ensure effective co-ordination of the strategy, the Lord Chancellor's Department should take overall responsibility for championing and overseeing implementation of the conclusions of this report – supported by the relevant organisations in specific fields (e.g. IDeA). It should provide a capacity to assist departments and other public sector organisations in modernising their information management strategies, facilitate resolution of inter-departmental issues, and build links with existing initiatives in electronic government and the overall modernisation of public services as described above. This will also enable greater alignment of data-sharing policy with policy on data protection.	This will be ongoing work for the Lord Chancellor's Department.	This is ongoing work, but a CKO – or equivalent role – should ideally be appointed immediately in the Lord Chancellor's Department, with a supporting team in place as soon as is practically possible. As with other organisations, functions should begin to be integrated further as soon as possible.
21.	To ensure better training for information management professionals, the Centre for Management and Policy Studies, working with training partners and drawing on best practice standards and guidance from, for example, the Public Record Office, should develop a series of training and education programmes for public sector officials involved in data-sharing and information management.	The Centre for Management and Policy Studies, which also has responsibility for the Civil Service College, should lead this work, building on courses already available and expertise in other organisations, such as the PRO.	Courses should be available by the end of 2002.
22.	Departments should consider how initiatives to support better data use can be mainstreamed within their existing financial plans and those that will be set as part of the 2002 Spending Review, building on e-business action plans as appropriate. In addition, e-business action plans – as part of wider business design – should address the issues of privacy protection and better use of data.	Financial planning is the ultimate responsibility of individual public services. The OeE will have a role with regard to e-business action plans. Broad criteria for good information management should also be applied at all assessment points, such as OGC gateway reviews.	Departments should look to mainstream data-sharing initiatives within existing financial plans as soon as is practically possible.
23.	The Lord Chancellor's Department should develop guidance on the interpretation of administrative powers and the key principles within the Data Protection Act with regard to how data-sharing can and should operate within the existing legal framework.	The Lord Chancellor's Department, working in partnership with other interested stakeholders, should lead this work, taking ownership of the guidance and ensuring it is widely available.	A first circulation of the legal guidance should be issued by the end of 2002, with updates following as appropriate.
24.	The Government should consult on the introduction of legislation to enable public bodies to share personal data with the consent of the data subject. This power would need to operate without prejudice to existing data-sharing gateways and practices.	The Lord Chancellor's Department, which has policy responsibility for data protection, should lead this consultation.	The proposals are published here for consultation. The Government would welcome responses by 14 June 2002.
25.	The Government should consult on change to enable data-sharing gateways to be established via secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny.		

ANNEX: THE ANALYTICAL FRAMEWORK[88]

What is it?

A.01 A strategy for advancing both data-sharing and privacy needs to be supported by a clear framework for decision making. Whenever the costs, risks and benefits of a policy approach are unfamiliar, diffuse and indirect or occur over different timescales, they are neither easily quantifiable nor comparable. Standard cost-benefit techniques are incomplete for the purpose. It is important, therefore, to have a clear process by which the costs and benefits can be identified and described.

A.02 An analytical framework – the full version of which is given at the end of this annex – has been designed to aid this process. It aims to condense the decision-making process into its basic steps. At each step, it attempts to define, by grouping into discrete types, the different benefits, risks and costs that may arise. By giving conceptual clarity to each of the different costs and benefits, the framework helps in developing ways of describing, measuring and adducing evidence to each. It also helps to identify remaining gaps in knowledge and methods and where more research and guidance would be useful.

A.03 The analytical framework reflects the principles that have been developed in the report and ensures that they influence departments' decision-making processes. The framework, by making explicit and emphasising the balancing question, "how large are the benefits of increased data-sharing *in relation* to the costs and risks?", and indicating how evidence for each may be gathered, aims to ensure privacy issues are fully considered at key stages in the decision-making process. The framework also asks questions about the practical measures that will ensure the net benefits identified at appraisal do indeed materialise.

A.04 The aim of the framework is to assist public bodies in considering the important questions surrounding better use of information in order to improve delivery of their objectives. The Lord Chancellor's Department should provide guidance and support, and will further develop both the analytical framework and related tools. The decision when to use the framework and other diagnostic aides will remain with service providers.

Why is it needed?

A.05 The analytical framework developed during the course of the report has been informally tested on three case studies,[89] and modified as a result. Overall, the departments concerned said that they found it an extremely useful tool. More generally, there is a demand in departments for analytical assistance of the sort provided by the framework: according to a MORI survey commissioned for this report, three quarters of civil servants with data-related responsibilities agreed that there were privacy

[88] See also Annex D published on the PIU website: www.piu.gov.uk/2002/privacy/report/index.htm
[89] NHS Executive, DWP (formerly DSS) and DVO Taskforce, DTLR (formerly DETR).

implications in their departments' plans for increased data-sharing; but they were divided on whether those implications would be positive or negative.[90]

A.06 A systematic checklist approach helps with the appraisal of any new policy where quantitative evidence is lacking. It is particularly valuable at this stage because it will:

- ensure a consistency of approach across government to considering privacy impacts;
- integrate the consideration of privacy costs and risks into a wider cost-benefit analysis;
- ensure an opportunity for unfamiliar, unanticipated and indirect costs and benefits of data-sharing to be identified;
- contribute to transparency; and
- constitute something of a systematic assessment of need which compliance with the proportionality requirement of the Human Rights Act implies.

When should the analytical framework be used?

A.07 The analytical framework covers the questions that need to be asked when a policy initiative, a business re-engineering process or an IT project encompasses any element of storing and using a citizen's data electronically, even if only as a minor part of the proposal. In summary, the question which should be kept in mind by all officials considering **any** new initiative is: *Does this policy imply the use of personal information – either new data or old data – for a new purpose?*

A.08 The question can be unpacked further:

- **Is the information being used for the original aim but in a different context?** For example, where a patient's GP notes are passed on to a hospital when there is a referral.
- **Is the information being used across departments to create a new service?** For instance, where an applicant for exemption from vehicle road tax on the grounds of disability grants DTLR permission to approach the Benefits Agency for confirmation of the disability and therefore does not need to apply for and present a certificate from the Agency.
- **Is the information being used for a completely different purpose from the original intention?** For example, where Inland Revenue data on incomes, collected for taxation purposes, is used when considering the seizure of criminal assets.

A.09 It will be important for public sector bodies to examine privacy issues as soon as a new policy initiative involving better data use or new data-sharing is mooted. This is the moment when there will be the fullest appraisal of implementation options for the policy. Options are very quickly narrowed down so it is important that the key privacy questions form part of this early, wide-ranging appraisal.

How should departments use the framework?

A.10 The framework should be used to guide the work of Chief Knowledge Officers (CKOs). It indicates the questions that they should ask their department in relation to all policy initiatives with data-sharing intentions. Answers to these questions would indicate when a full privacy impact assessment is

[90] *Attitudes towards data-sharing: a survey among civil servants*, MORI research study conducted for the Performance and Innovation Unit, November 2000 – January 2001.

called for. The framework asks six basic questions:

i What is the policy objective?

ii What are the benefits of the proposed data-sharing?

iii What kind of data-sharing is proposed and what are the alternatives?

iv What are the costs and risks of data-sharing?

v How large are the benefits in relation to the risks?

vi What is being done to maximise the benefits and minimise the costs and risks?

What is the policy objective?

A.11 Specifying the overarching goal to which it is proposed data-sharing will contribute is the first step in clarifying the department's thinking, and should be borne in mind throughout the stages that follow. It is also a first step in challenging any prejudices or presumptions about the data-sharing solution. Early clarity about the goal of policy will prompt early consideration of alternative solutions.

What are the benefits of the proposed data-sharing?

A.12 It is often assumed that data-sharing is synonymous with more knowledge and therefore needs little justification. But this fails to specify and ultimately balance the benefit against the costs. Current government policies lead us to specify three distinct areas of benefits: better services to citizens; better targeted policies; and better value for the taxpayer. Being able to define these three distinct types of benefit not only enables us to move onto another level of specificity and take another step towards quantification but it makes clear that some types of benefits will be felt directly by citizens as consumers of services, others will be felt indirectly as taxpayers and some will be felt indirectly as the beneficiaries of government policies. This is important because where benefits fall affects how risks are perceived.

What kind of data-sharing is proposed and what are the alternatives?

A.13 There are different kinds of data-sharing. Of the pure data-sharing *between* departments there are two kinds: a) case-by-case sharing between departments and b) batch database matching between departments; these have quite different cost, privacy and procedural implications and this needs to be made clear and understood. Data-sharing may also involve anonymised data or be compulsory or voluntary. There are other approaches to more and better use of data that are not exactly data-sharing but they are alternative ways of combining and improving data use that should be considered, again because they have different costs, benefits and legal, *vires*, implications.

A.14 An important alternative is the better use of a department's own information through sharing *within* a department. It is clear that many departments and local authorities are not aware of the extent of the data held within their own borders, nor have they given proper consideration to the opportunities of rationalising and combining the databases they already have. While consent and compliance with the Data Protection Act remain an issue, a statutory facility to share and combine data may

already exist; and there may be added administrative efficiencies in taking this approach. There are also likely to be added costs, and data-sharing with another department may be a rational – though implicit – alternative to the internal organisational changes that are entailed. For rational decision making, this needs to be made explicit.

A.15 Other alternatives to departmental data-sharing are: collection of new data; use of publicly-available data such as the electoral register, lists of postcodes or land ownership registers; and the use of private sector data such as might be purchasable or accessible from credit reference agencies and direct marketing companies. The costs, benefits and privacy risks of each of these options need to be compared.

What are the costs and risks of data-sharing?

A.16 This is an important area for CKOs to focus on. The technical, organisational and legal costs of more information use are relatively new and unfamiliar territory for government. Even the private sector still has a long way to go in defining and quantifying them. Assistance in defining and measuring costs and risks will be an important contribution to identifying the most effective policies. We have broken down the costs specific to data-sharing as:

- **Legal costs:** Any new use of personal information must comply with data protection legislation, but there may be combinations of alternative data sets which already have consent which do not have to be repeated. The first data protection principle requires that any processing of personal information must be legal and all sharing across departments requires statutory permission. The costs – mainly in the seeking of legal advice, consulting and awaiting a legislative slot – of gaining the statutory permission for new data-sharing powers should be weighed against alternative approaches to gaining the same information from other sources.
- **Sharing costs:** Again, as a new activity for many departments, the costs of sharing data may not be obvious, nor direct. But they can be substantial and so need to be signalled and efforts made to quantify them at an early stage. The sharing costs we have identified so far include the necessary minimum standardisation to permit effective sharing; measures necessary to counteract any expected deterioration in data quality as a result of the sharing; possible changes in voluntary compliance levels by the public as a result of awareness of more data-sharing by government; and any sharing by one department of the uncompensated costs of another.
- **Safeguard costs:** In the main body of the report we argue that public concerns about increased data-sharing by government are likely to require data-sharing to be accompanied by special privacy safeguards. These may be either technical – privacy enhancing technologies – or staff based. These staff costs may include new general staff training or specific arrangements to limit staff access that may be necessary to ensure safe handling.

A.17 Perception of, and response to, risk are of increasing interest to policy makers. How to assess risk, how to incorporate it into project and policy appraisal, and how to weight and factor in public perceptions of risk are still an inexact science. The project's public attitudes research[91] confirms existing

[91] *Strategies for Reassurance: Lessons from Focus-Group Research on Allaying Public Concerns about Privacy and Data-Sharing in Government*, Perri 6 (Cabinet Office, February 2002). See also *The future of privacy* by Perri 6 (Demos, 1998).

conclusions that risk is an important determinant of public perceptions. The public tends to be sceptical that it will see the theoretical benefits, either because it has understood the well publicised difficulties around large government IT investments or because it believes benefits to be extracted elsewhere in the system.

A.18 The public may also have a different understanding to that of departments of the risks attached to such privacy-related issues as security and confidentiality. It is important for public services, when proposing to increase data-sharing, to check whether their perceptions of risk are in line with the public's and to understand the implications of any differences. They could be significant – for instance, a slower take-up of on-line services or a decline in voluntary compliance.

How large are the benefits in relation to the risks? The balance

A.19 It may seem simplistic to ask that benefits be balanced against costs and risks. It is difficult to quantify each of these three aspects separately, and it is even harder to compare them against each other. Nevertheless, this section of the framework is intended both to emphasise this balancing process and to support departments in undertaking it. It breaks the process down into a number of more manageable considerations:

- How large are the barriers to data-sharing?
- What are the attitudes of consumers and citizens?
- What can be learnt from similar projects in the public or private sectors?
- What are the consequences of failing to communicate the risks properly?
- What are the consequences of unauthorised access, poor data quality etc?
- How vulnerable is the IT to technical failure, security breaches etc?

What is being done to maximise the benefits and minimise the costs and risks?

A.20 Having concluded that the balance between costs and benefits is in favour of going ahead with the proposal, there remains one more step in the analytical framework: when the proposal is implemented, efforts to minimise the risks and costs and maximise the benefits should continue. The previous stages of the framework will have been conducted on paper – a desk-based analysis. This stage aims to make privacy-promotion real.

A.21 The detailed design of the processes and systems to support the proposal must deliver privacy commitments as well as achieving service-related objectives. By asking this final question, the framework requires specific answers about safeguards to be put in place to protect privacy – such as privacy-enhancing technologies – and about actions to build confidence in data-sharing arrangements – such as data quality assurance mechanisms and external scrutiny.

The role of a privacy impact assessment (PIA) in the analytical framework

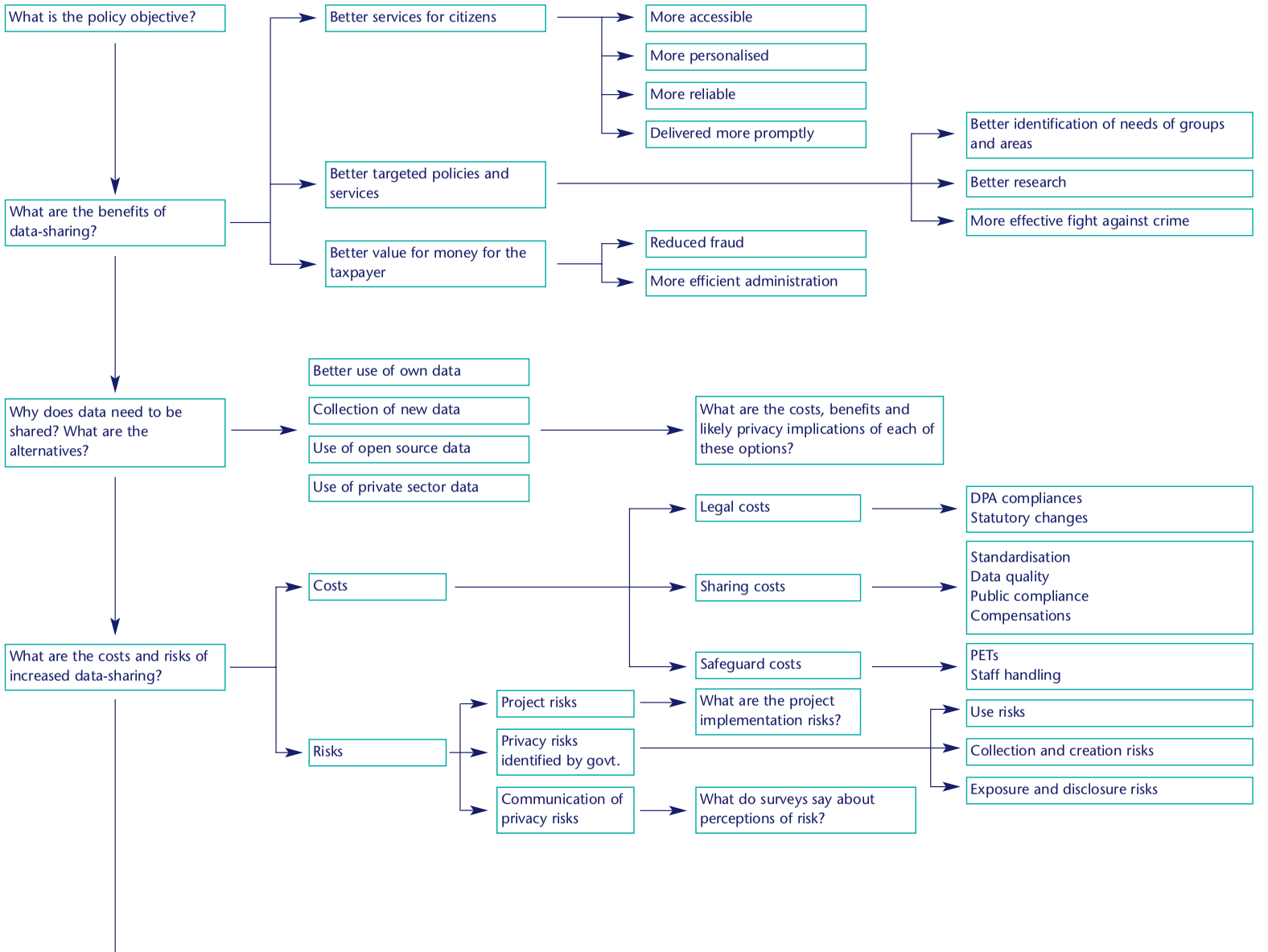
A.22 The analytical framework considers the balance between the benefits arising from greater use of data, the costs of the proposal

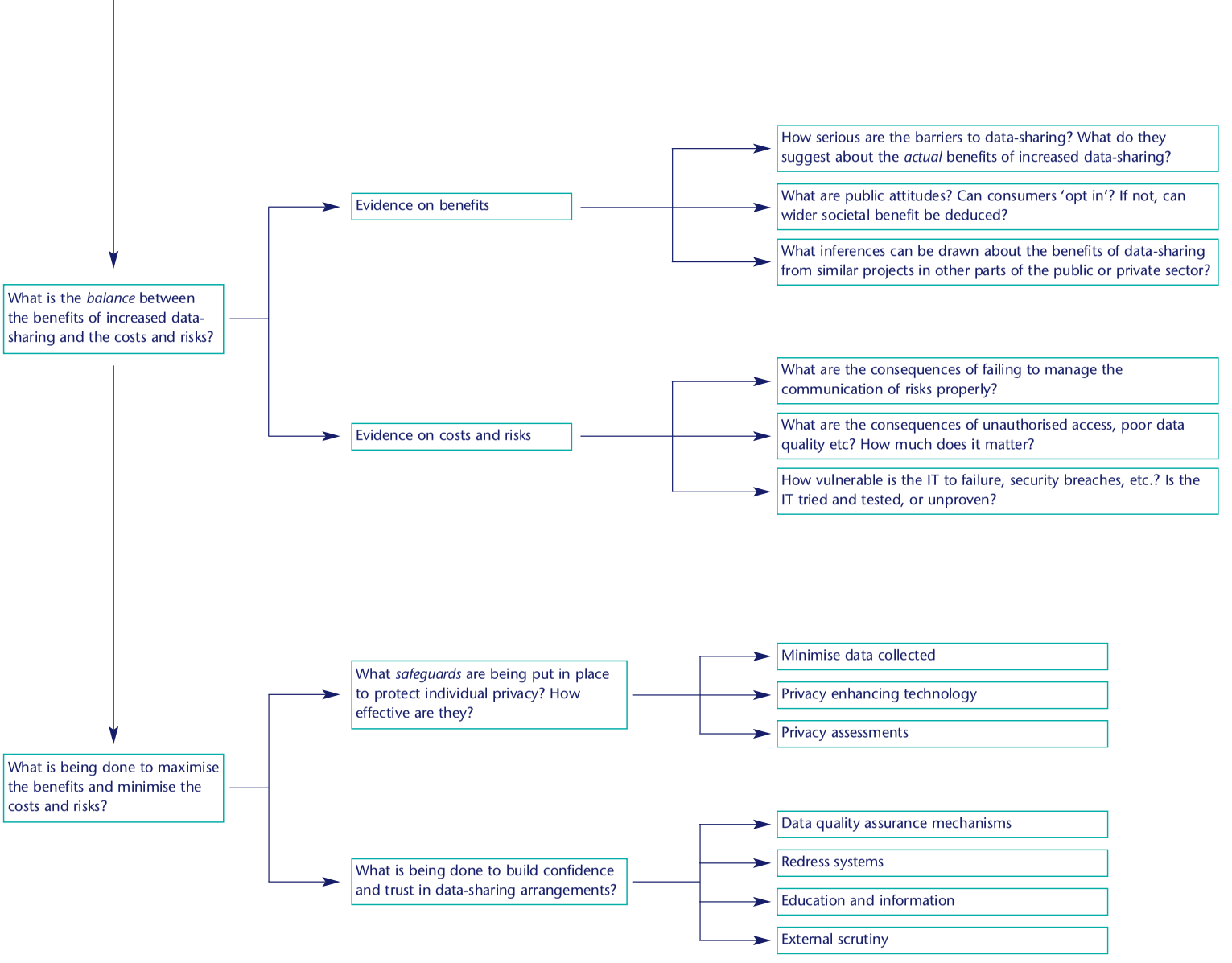
and the risks, including privacy risks. There are well established methodologies for assessing financial impacts and for assessing technical risks which can be used to feed information into those sections of the analytical framework. Until recently, there has been no equivalent method to assess privacy impacts and risks. This report demonstrates how complex and wide ranging those privacy issues and risks can be, and how important an equivalent methodology will be in giving privacy issues a fair weight in the balancing process. Privacy impact assessments have been developed elsewhere to fill this gap.[92]

Further development of the analytical framework

A.23 The outline of the framework given here provides a structure on which information managers can build. Experience of using it should lead to improvements. If the processes prove too burdensome or inappropriate in some cases they should be modified and developed.

[92] e.g. *Privacy Impact Assessments for Justice Information Systems*, US Department of Justice Working Paper, August 2000; *Privacy Impact Assessments*, Blair Stewart, in *Privacy Law and Policy Reporter* volume 3, number 61, 1996.
See also www.oipcbc.org/publications/pia and www.anu.edu.au/people/Roger.Clarke/DV/PIA.html


What is the policy objective?
What are the benefits of data-sharing?
Better services for citizens
More accessible
More personalised
More reliable
Delivered more promptly
Better targeted policies and services
Better identification of needs of groups and areas
Better research
More effective fight against crime
Better value for money for the taxpayer
Reduced fraud
More efficient administration
Why does data need to be shared? What are the alternatives?
Better use of own data
Collection of new data
Use of open source data
Use of private sector data
What are the costs, benefits and likely privacy implications of each of these options?
What are the costs and risks of increased data-sharing?
Costs
Legal costs
DPA compliances
Statutory changes
Sharing costs
Standardisation
Data quality
Public compliance
Compensations
Safeguard costs
PETs
Staff handling
Risks
Project risks
What are the project implementation risks?
Privacy risks identified by govt.
Use risks
Collection and creation risks
Exposure and disclosure risks
Communication of privacy risks
What do surveys say about perceptions of risk?


What is the *balance* between the benefits of increased data-sharing and the costs and risks?
Evidence on benefits
How serious are the barriers to data-sharing? What do they suggest about the *actual* benefits of increased data-sharing?
What are public attitudes? Can consumers 'opt in'? If not, can wider societal benefit be deduced?
What inferences can be drawn about the benefits of data-sharing from similar projects in other parts of the public or private sector?
Evidence on costs and risks
What are the consequences of failing to manage the communication of risks properly?
What are the consequences of unauthorised access, poor data quality etc? How much does it matter?
How vulnerable is the IT to failure, security breaches, etc.? Is the IT tried and tested, or unproven?
What is being done to maximise the benefits and minimise the costs and risks?
What *safeguards* are being put in place to protect individual privacy? How effective are they?
Minimise data collected
Privacy enhancing technology
Privacy assessments
What is being done to build confidence and trust in data-sharing arrangements?
Data quality assurance mechanisms
Redress systems
Education and information
External scrutiny

Performance and Innovation Unit
Cabinet Office
Fourth Floor
Admiralty Arch
The Mall
London SW1A 2WH
Telephone 020 7276 1416
Fax 020 7276 1407
E-mail piu@cabinet-office.x.gsi.gov.uk
Web www.piu.gov.uk

Publication date April 2002

This report is printed on Revive Matt material. It is made from 100% recycled post-consumer waste, is totally chlorine free and fully recyclable.

Ref: CABI J01-9063/0402/D16