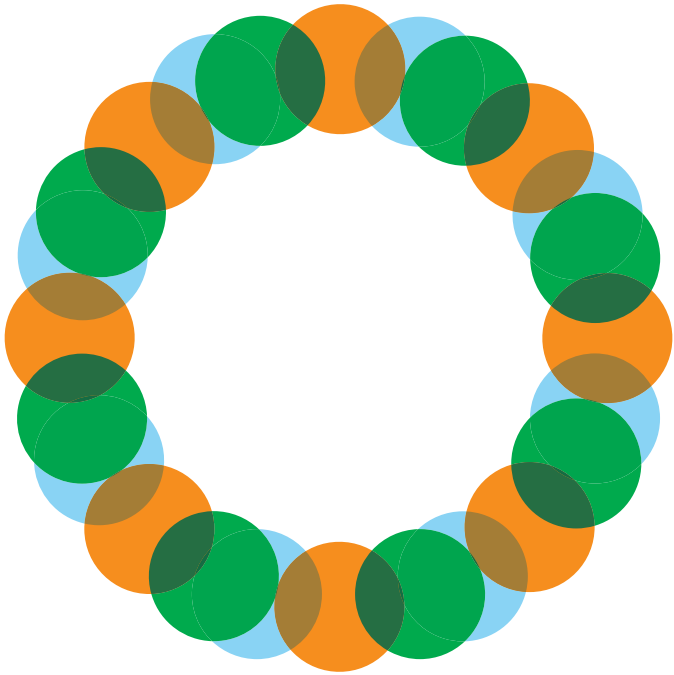
Who shares wins? Transforming the public services with intelligent information

Alex Karalis Isaac and Claudia Wood



The Social Market Foundation

The Foundation's main activity is to commission and publish original papers by independent academic and other experts on key topics in the economic and social fields, with a view to stimulating public discussion on the performance of markets and the social framework within which they operate. The Foundation is a registered charity and a company limited by guarantee. It is independent of any political party or group and is financed by the sale of publications and by voluntary donations from individuals, organisations and companies. The views expressed in publications are those of the authors and do not represent a corporate opinion of the Foundation.

First published by
The Social Market Foundation,
October 2006

The Social Market Foundation
11 Tufton Street
London SW1P 3QB

Designed by www.jadedesign.net

Contents

Overview **4**

Executive Summary **6**

Introduction **15**

Section One – Three Fundamental Challenges **18**

Chapter 1 – To share or not to share **19**

Chapter 2 – Privacy, technology and an information society **30**

Chapter 3 – The law – barrier or safeguard? **47**

Section Two – Practical And Technical Challenges **63**

Chapter 4 – Joining up government **65**

Chapter 5 – The new localism? **75**

Chapter 6 – Managing relationships **91**

Conclusion **107**

List of Abbreviations **110**

References **112**

Overview

The government is developing a new information policy. This new policy must work for modern society in which expectations of public service efficiency and quality are high, information is (potentially) digital and people are highly mobile. However, the existing information handling environment originated in an earlier ration-book era, and is increasingly unfit for purpose. The Cabinet committee on data sharing, MISC 31, charged with developing this new strategy, will seek an information culture which can allow improved delivery, efficiency and security. However, the committee must also develop an information sharing system which protects personal privacy and avoids the potential inefficiencies of too much information sharing.

Arriving at such a policy will require a sophisticated debate and an understanding of both the benefits and the risks of improved government data sharing. Currently, information is scattered haphazardly across separate agencies with no regard to the reality of how citizens actually interact with the state. This inflates costs and introduces scope for fraud and error. On the other hand, sharing data between departments can be hugely expensive and time consuming, and requires constant security and quality management. A balance must therefore be struck – we must make progress towards a coherent and efficient use of information across government, without going too far and creating new inefficiencies or compromising individual rights. This balance may pivot on an assessment of the potential costs and benefits of individual instances of sharing data. Only when such an analysis can be made will government be able to utilise modern technology and ensure it does not slip irredeemably behind the private sector in terms of efficiency and service quality.

During this project, the SMF team has sought to identify

where this balance might lie, proposing a set of policies that can simultaneously advance the scope of data sharing while ensuring personal information remains only in the hands of appropriate professionals. We have reviewed a wide range of domestic and international evidence to define key challenges and suggest solutions. We have held a series of expert seminars, covering international and domestic experience and potential policies, to further inform this process.

Executive Summary

There are very few activities in our modern lives that can be undertaken without the movement of information from one place to another including travelling, working and many leisure pursuits. For the most part, the multiple processes involved are taken for granted, and only noticed when something goes wrong.

Nowhere is this truer than in our interactions with government. For all public services – healthcare, education, housing, criminal justice, benefits and taxation, etc. – to work, a range of public servants and agencies need to use our personal information in concert. Although these services have an impact on nearly every aspect of our lives, the information processes which drive them are unseen and taken for granted. Yet when these processes break down – and information is misplaced or incorrect – this can carry huge implications. Our benefits might not be paid into our accounts, our GP records may not get to the hospital we are being treated in, and so on. At best, this leads to inconvenience. At worst, mis-managed information can endanger our lives.

Despite the fact that poor information management by government can have a huge impact on our lives, government still does not use information very effectively. And this is against a background in which our expectations are growing – in other areas of our lives we can take advantage of increasing convenience facilitated by the Internet, swipe cards and other technologies. The government is falling ever further behind the private sector in terms of making information support customer interactions, combating fraud, and processing information efficiently.

If the government is to keep pace with the private sector

on service quality and the accuracy of delivery, as it must to maintain support for public services, information can no longer be stored in bureaucratic isolation. Information flows need to reflect the reality of citizens' multi-departmental interactions with government. Fortunately, this so far neglected aspect of public service reform is finally being challenged: the publication of *Transformational Government* called for increased data sharing to drive better and more efficient service delivery; the green paper *New Powers Against Organised And Financial Crime* calls for better use of information to tackle fraud and security risks; a cabinet committee, MISC 31, is working on a new information sharing framework to enable these transformations; and the recent Vision Statement on information sharing sets out a constructive direction of travel.

But this welcome and long overdue focus on improved information use by government brings risks as well as opportunities. For example:

- If the government enables too much data sharing it will create new inefficiencies and it may compromise our freedoms.
- If the government fails to empower the citizen, an opportunity to create a responsible and effective information society will be lost, and the government will face the possible rejection of its policies in the face of civil liberties opposition.
- If the legal framework, or at least the general interpretation of existing law, is not reformed to match information policy aspirations, then new policies will be stillborn.
- If informational integration is pursued in isolation it will fail – other government processes (such as funding and performance management) need to keep pace with any concrete action to 'join up government'.
- If central government does not offer sufficient leadership to drive this agenda, its vision will suffer patchy implementation and incompatibility. On the other hand, if there is too much central direction the risks of stakeholder rejection will multiply and compromise efforts to share information.
- If departments do not have effective structures for managing cooperative relationships, closer information sharing will create more dangers than it solves.

This report sets out a framework for overcoming these risks and transforming the function of information in government – from a source of administrative inefficiency into the lifeblood of more effective service delivery.

We start building this framework with three key principles:

- information sharing should deliver clear benefits to citizens using public services
- case-by-case assessment of the right to share data is too cumbersome to allow meaningful information sharing
- individual rights should be maintained or strengthened by the new information framework.

Building on these principles we can lay the foundations of a just and effective information society. The following report explores potentially problematic areas that must be resolved before government can implement an effective information strategy. Below we outline these areas and our proposed solutions:

Policy proposals

1) The extent of data sharing

- Parliament should pass a bill to establish the power of departments to share data where they can identify clear benefits to a particular shared user group, and present this case to scrutiny.
- Cases for data sharing should be assessed by a regulator, against the requirements outlined by parliament in a data-sharing bill – requirements that data sharing benefits the citizen and that individual rights are maintained or enhanced (see also bullet four, section three, below).
- Public servants covered by a successful case would not need further permission or legislation to undertake the data sharing described by the successful proposal.

2) New technology and the demand for privacy

- As far as possible people should have the right to choose whether or not to allow their data to be shared by a particular group of public servants. We would expect this to be a right included in a data-sharing bill.
- We should build on the Freedom of Information (FOI) framework, to give people increased knowledge of how their information is being processed:
  - if possible people should have access to the audit trails created when public servants access their data
  - within each department, there should be a single point of contact, to investigate allegations of miss-use of data, and sanction anyone abusing data-sharing powers.

3) The legal framework and cross-departmental data sharing

- Administrative law must establish the power of departments to share data to enable another department to discharge its duties. These powers should reflect the identification of cross cutting user groups, suggested above.
- Data Protection Act (DPA) guidelines should be revised to emphasise the possibility of data sharing between practitioners contributing to a clearly identified, justified purpose.
- Central departments and their agencies should develop roles similar to the "Caldicott Guardians" who oversee data sharing in the NHS and social services.
- A further role for the Information Commissioner's Office (ICO) (or other regulator) could be developed from the French model; this would allow the ICO to assess the benefits of service improvements against potential risks to privacy, rather than just assess legal compliance. ICO powers to block projects could be increased to ensure their continued independence (see also bullet two, section one, above).

4) Interdepartmental cooperation and budgets

- Budgets for interdepartmental cooperation should be ring fenced.
- Competitive tenders for additional funding would be the best way to organise any new funds for new cross-departmental projects.
- The evaluation of proposals for more funds will require the cooperation of specialists from the cross-departmental institutions including parts of the Treasury, Cabinet Office and possibly the National Audit Office.
- Public service agreements (PSAs) need to reflect cross-departmental priorities, and specifically the role of data sharing in meeting these. PSAs relating to data sharing should measure outcomes such as transaction time, or complaints levels, not the

mere process of exchanging data.

5) Reconciling central leadership and local enthusiasm

- Any large future projects will need to explore the middle ground between completely centralised delivery – recently heavily criticised – and the former status quo, of excessive localism and lack of progress on national priorities.
- Central government should develop its role as a centre of expertise in identifying citizen benefits from data sharing, and building the organisational models capable of realising these.

6) Challenges of data transfer and relationship management

- The government needs a clear mechanism for arranging compensation between departments saving money and departments incurring new costs through data sharing. This could be achieved via a price structure, or via Treasury adjustments to departmental budgets.
- For particularly important types of data, it would be useful to establish PSAs on data quality with the departments responsible for this information.
- Governing data quality will require appropriate Service Level Agreements and Terms of Use agreements between sharing departments.
- These agreements will need monitoring and enforcement from an agency capable of assessing the quality of information departments provide to each other. In the text we discuss several options for the location of such powers.

Exploring our proposals in more detail:

Civil society and information sharing

Parliament must legislate to define the circumstances in which practitioners can share sensitive data to improve services. Government departments should pursue their customers' interests through these new powers, and build business cases to demonstrate how their information sharing will improve services and improve individual information rights. A regulator – possibly the Information Commissioner – should ensure that these plans conform to the framework defined by Parliament. Practitioners should then be aware of their right, indeed their

responsibility, to share information under any certified proposals. Finally, service users and the public should exercise new powers of choice and oversight to enhance their experience of government and ensure practitioners are using data responsibly.

Customer groups and the extent of data sharing

A successful information sharing policy must try to define an optimum degree of data sharing, though this may vary for each individual citizen, which complicates the task. We believe that this degree can be identified by using the nature of citizen interaction with the state as the basis for information sharing. For example, an individual may use taxation and benefits systems at the same time and within the same context. Alternatively, a particular type of case may require the joint effort of social and health services and the police. Where such cross-cutting customer groups and cases can be identified, practitioners in the relevant services should be able to share information. This power should be subject to the development (at the agency or department level, not the individual level) of a suitable business case, which demonstrates the benefits of sharing within those cases or for those individuals, and which also ensures that information remains only with those who need to know it. In addition, there should be a mechanism for the public evaluation of such business cases against the criteria of primary legislation, which should define a process for the identification of suitable customer groups.

Some large similar services will be able to identify large overlapping customer groups and demonstrate a strong business case accordingly. The transactional services would be an example. In most cases however, customer groups will be much smaller, interacting with select professionals in a range of services. The users of Children's Centres would be an example of this. Such information sharing will not require much IT, but it will require a clear public mandate for public servants to share information.

Trust and the law

Trust is critical to successful interactions and the efficient flow of information. We suggest that trust is the best basis for interaction between citizens and public servants who have the power

to share their data. This trust can only be developed if users can exercise, wherever possible, personal choice, and also have power to oversee the actions of those who handle their personal data. Freedom of Information legislation takes a first step in this direction, but an effective information society will go further. It will allow individuals to review audit trails for their data to ensure those who access and use it are doing so for legitimate purposes. It will also allow, in most circumstances, the citizen to opt in and opt out of data sharing practices depending on how highly they value access to improved services.

Law has a crucial role to play in regulating the data-sharing environment. We believe that law is the appropriate safeguard against abusive behaviour – by the state or anyone else. However, legal complexity is not the best way to regulate the use of data; case-by-case analysis of powers to share data stifles the use of information on the ground. We should recognise the role of law in protecting us from abuse, but law is not a substitute for developing trust.

We should ensure that we understand and use the powers available to democratic governments to pursue their legitimate aims under the law, including the power to pursue sensible data sharing. We feel the approach outlined in this paper is consistent with both the Human Rights Act and the Data Protection Act. Administrative law is more complex. Establishing the power to share data, without compromising the separation of government departments, is certainly possible, but may require even more work than making people aware of the possibilities for data sharing contained in the Data Protection Act.

Joining up government

Data sharing is part of 'joined up government' and it cannot be pursued without other measures to join up government processes. Particularly important will be the adaptation of departmental budgets to facilitate co-operative working, and the development of sensible Public Service Agreements to incentivise information co-operation. The use of competitive access to additional funding could be a powerful incentive to establish co-operation where it has not previously existed. At a minimum we must ensure that budgets for co-operative working are protected from diversion into better-established priorities. Sensible PSAs

governing data sharing will focus on the desired outcomes, not on the process of data sharing. They may measure transaction time, the level of complaints, or the accuracy of delivery, but they should not stipulate volumes of information movement.

Balancing local and central authority

To pursue data sharing effectively, especially when delivering large projects, government will need to refine the roles of central authorities and local stakeholders. This is a specific example of the wider debate surrounding central power and local responsibility. We believe government has made much progress in this area and future projects will only learn from the difficulties experienced by Connecting for Health. Further thinking about precisely how much responsibility can be devolved to the local level will be useful, though some power must remain in the centre to direct budgets and define the limits within which local institutions can pursue their own priorities. We also believe that central government should develop a centre of expertise in identifying and valuing the benefits of data sharing, and make this knowledge available to departments as they build business cases for data sharing.

Data quality and data sharing

Efficient data sharing will require the management of cross-cutting responsibilities and interactions on a far greater scale than has previously been practiced in government. Responsibility for data quality processes must be decided between parties and they must face contractual obligations to maintain and monitor these actions. There is little suitable machinery for such contracting, but it must be developed if we are to guarantee data standards in data sharing systems. PSAs can mandate the creation of such contracts, but to be successful such contracts will need to be owned by the sharing bodies, not by an outside institution.

Conclusion

Although the achievement of efficient information sharing processes within government is beset by many challenges – structural, organisational, and cultural – the potential gains for both government and the individual citizen are enormous. Not only is this a reason not to be discouraged by the difficulties that

lie ahead, it is also one method of overcoming them. With a suitable focus on customer benefits, combined with enhanced information rights, good management and technical expertise, government stands a good chance of building on the positive work contained in Transformational Government and the information sharing Vision Statement.

Limits of this report

In this report, we consider the sharing of personal information between government departments – the most politically charged and problematic form of data sharing. However, this is just the tip of the iceberg – there are many other forms of information which the government does share and could improve upon – aggregate locational information, geographical information, anonymised information for research, and so on.[1] These already do deliver real benefits to citizens, from GPS systems using Ordnance Survey information to guide drivers around traffic jams, to more effective social policies based on accurate information about current and future demographic trends. Although we do not explore how the government could improve its management of such information here, we should acknowledge the significant potential benefits available from it. In addition, using this information – which tends to be anonymised and aggregated and therefore fairly uncontroversial – could be an excellent way to trial the technologies and governance mechanisms required to share personal information more effectively, but with fewer risks to individual privacy. In addition, demonstrating the real convenience and efficiencies that can be delivered by joining up these relatively uncontroversial types of data, we may be able to pave the way for greater public acceptance of wider use of personal data to deliver efficiencies in other areas.

1 For further analysis of the problems and opportunities available in exploiting this resource see Office of Public Sector Information, www.opsi.gov.uk and the Advisory Panel on Public Sector Information, www.apsi.gov.uk

Introduction – what is data sharing and do we need more of it?

What is data sharing?

Put simply, data sharing is one part of government telling another what it knows, often about a particular person. However, this rarely happens – despite government pronouncements, individual governments are not very "joined up". *Transformational Government,* suggested that we need to see a lot more data sharing in the future, so that government departments can share their corporate services and improve their front office interactions with service users. Recently, the Home Office has issued a green paper, *New Powers Against Organised and Financial Crime,*[2] suggesting we need more data sharing to combat criminal activity, from fraud to terrorism. In short, the more government departments know, the better they can deliver services, from benefits payments to counter terrorism operations.

Of course, delivering services means influencing people's lives. This may not always be a good thing. Can government be trusted only to deliver services which improve people's lives, or will they use this power to destroy personal freedom? Can government employees be trusted to use data responsibly, or will they sell it on for personal gain? The more data sharing happens, the worse these destructive possibilities might be. Some groups such as *Privacy International*[3] are very concerned that these risks are large, any benefits small, and any more sharing is an attack on personal freedom.

As a consequence, public debate has been very polarised – privacy groups portray all data sharing as a threat to liberty

2 http://www.homeoffice.gov.uk/documents/cons-2006-new-powers-org-crime/cons-new-powers-paper?view=Binary#

3 http://www.privacyinternational.org/

while the government refuses to acknowledge legitimate concerns. It is essential we get away from this polarisation and attempt to discover how data sharing can be used to create better government, not bigger or more powerful government.

How much data sharing do we need?

Currently there is too little data sharing – money is wasted and lives are lost as a consequence. For example, £1.8bn in tax credits was overpaid last year because of deficiencies in HMRC's information;[4] up to 6p in the pound may be paying for fraud in the public sector[5] and dangerous prisoners have been mistakenly released because probation and prison services do not automatically or reliably update each other's records.[6]

However, the recent difficulty of the ID cards programme arose because the data sharing proposed in some versions of this scheme was potentially more of a threat than a benefit to citizens. While we support more data sharing, we do not support *all* data sharing. The ID card database, for example, could have been a security threat and a threat to liberty, revealing unnecessary personal information and delivering few benefits to citizens in return. It is no longer clear that the ID card programme will involve the construction of a new database.

Rather, we are seeking to achieve an optimum level of data sharing that allows government services greater accuracy and efficiency than they currently achieve, but which does not threaten personal freedom by revealing information to people who do not need to know it. This is described below.

4 *NAO Comptroller and Auditor General's Standard Report on HMRC 2005-06 Accounts,* p R2

5 Counting the cost of UK fraud, 24 November 2005 http://news.bbc.co.uk/1/hi/business/4463132.stm

6 See for example http://news.bbc.co.uk/1/hi/uk_politics/4942886.stm

For each individual this function will be different. Some of us value our privacy very highly indeed, while others particularly value the efficiency of government services. Every individual will have an individual optimum. To find an optimum level of data sharing, it is not enough to ensure that information remains only with those who need to know it – there must also be some room for individuals to personalise their information relationship with government.

The following report attempts to outline a set of policies which the government can pursue to make progress towards optimum sharing, while ensuring it does not stray beyond this and waste money or compromise individual freedom. The focus is on providing the right information to the right people, so that they can perform their publicly mandated tasks to the best of their ability, at least cost to the taxpayer. We advocate more data sharing, but we advocate strong conditions governing the extent of this sharing, and pay a great deal of attention to mechanisms by which the government can increase the public's oversight of their data and improve people's rights as data-citizens in an information society.

Section One – Three Fundamental Challenges

Chapter One: To share or not to share – the extent of data sharing

Introduction

The government intends to pursue data sharing to improve the efficiency of services and to improve the quality of services available to users – making processes faster, less bureaucratic, and more accurate. We support the concept of using data sharing to make government work better for citizens, and believe that this mission should define the extent of data sharing. Any consideration of this topic quickly arrives at the following question:

Do we need a single solution for the whole of government, or should we seek only to join up information flows between particular clusters of government agencies?

To answer this question we must ask how data sharing can improve customer experience and consider some of the technical differences between whole-of-government and more limited solutions. The benefits delivered by the Criminal Justice IT Unit (CJIT) and Connecting for Health (CfH) will be helpful in this.

Whole-of-government solutions vs. part-of-government solutions

Collecting and holding data is expensive. There are, therefore, significant potential cost savings to be had from the central coordination of basic demographic data. This could be organised through a central database, analogous to the NHS SPINE. Alternatively responsibility for disseminating basic demograph-

ic data could rest with a designated department(s) which routinely deals with such information. However, while efficiency gains – for government and for people supplying their details to government – would be large, such a system would create a need for a universal identifier of basic demographic data. A universal identifier could create a security concern, where different sets of records are accurately matched to this identifier across the population. Such an identifier would make it easier to match different types of records to relating to a particular individual. However, it would not become any easier to actually gain access to the separate databases where more sensitive information would continue to be stored. Therefore this security concern may be small (we should remember security is often a human rather than a technical problem, arising through corruption or deception). If the security concern is indeed minimal, the potential efficiencies available may encourage government to pursue one integrated approach to basic demographic data.

However, it is certain that we do not need to centralise the storage of more detailed, process-specific information in order to enjoy the benefits of better and more efficient delivery. To do so would create real security and civil liberty concerns. We need an alternative approach for the great majority of sensitive personal information.

The cluster approach

Communication *between* existing departments will be crucial to future efforts to join up services across administrative boundaries. This could be achieved either by a single solution, enabling any part of government to communicate with any other part, or by a series of different solutions enabling communication between specific parts of government. How much more data sharing do we wish to see? To answer this logically, we should ask: what kinds of data sharing can lead to service improvements, and what kind of data sharing can save public services money?

Giving public servants access to improved information can lead to greater transactional efficiency and better decision-making – these are both significant service improvements. Second, information is expensive to acquire, store and update. Rationalising the collection, storage and maintenance of information will free resources from administration and direct them towards delivery.

Therefore, service improvements are likely to be available where disparate agencies share responsibility for the successful conclusion of a given case, and cost efficiencies can probably be achieved where different agencies are collecting and processing the same information on a regular basis.

We can illustrate this potential for improved delivery and improved efficiency by considering how data sharing between departments could affect the experience of a benefit claimant:

Consider someone who has become unemployed, left their hometown and moved to a city to seek work. They will need jobseekers allowance, housing benefits and may be eligible for tax credits on any income they do secure. This person moves around their new city frequently at first. Repeating their life story and completing new forms at each new office of all the above agencies will be frustrating and time consuming. It may also be distressing to constantly review difficult experiences such as becoming unemployed. Delays in these processes will cost the claimant money. This is a serious problem – food and shelter are basic commodities and when they are beyond reach because of administrative delays this is a serious service deficiency. The more often data must be re-entered into the system, the more often forms must be filled in and procedure completed, the greater the risk that service delivery will be compromised.

It would be better if this person's case information were available to public servants as required. Once someone has registered their details for the purpose of receiving benefits, these details should always be available for receiving benefits, as long as that person continues to need such service. If all of these transactional services (HMRC, DWP, local authorities) shared information, the individual would experience a far swifter, more convenient and more reliable process in moving to a new location. This would be a significant benefit to the individual, reducing the burden of interacting with government and freeing more time for finding work and accommodation.

Therefore, sharing data between a cluster of departments who all serve a particular individual may significantly improve the service. In addition, this improved efficiency could also translate into large cost savings for government departments

through improved efficiency. For example, DWP and HMRC both require names, addresses, incomes, employment details, family status and assets information in order to administer taxes and benefits. Yet both collect all this information and attempt to keep it up to date individually. Potentially, removing this duplicated effort would save considerable resources. As both departments already have this information, and use it for the purpose of administering transactions, their sharing data would neither increase the information the government holds about a citizen, nor contravene the Data Protection Act. But it would make their services more reliable *and* more cost effective.

In this case we have identified one process – transactions with government – which is divided across government departments, introducing unnecessary risk and cost for service users and the departments concerned. We have also identified one very large customer group – benefits users – whose experience is unnecessarily compromised because the divisions between government departments do not accurately reflect the reality of people's interaction with government.

Helping a victim of domestic violence is another where data sharing can improve quality and efficiency of services. First, the police must provide protection and pursue the perpetrator. Medical intervention may be required to help the victims, and later medical evidence will be crucial to the conviction. The local authority housing department may also have to provide sheltered accommodation and keep its location secret. Simultaneously, social services may be required to provide support. If a child is involved, that child's education records may have to be transferred between schools, but again this may have to be done without alerting the perpetrator – which will require knowledge of the case.

This is clearly a very complex set of interactions with the state. For the victim in question, continually providing information to this myriad of agencies will be extremely time consuming and distressing. The repeated information gathering of the various agencies will introduce delays in service provision and increase the risk of error. Both delay and error in this case could have serious consequences.

A much-improved service would be achieved if the professionals dealing with the case in each of the above agencies could share necessary information with each other. At the moment, this may only be the case between the medical services and the police to secure a conviction. If authorised members of each service were to be able to share relevant information in every one of these transactions, with authorisation restricted to relevant caseworkers, this would increase the speed with which the victim could be re-housed and resettled, and the perpetrator prosecuted, with commensurate benefits to public safety.

In this example, there is not a large customer group, and there is not typically much overlap in the nature of the services involved. Nevertheless, this type of complex, multi-agency case would be hugely improved if selected case workers in relevant authorities could communicate when such cases arose. Undoubtedly there is a clear customer group here – the victims of domestic violence – and it would be extremely useful if the state could act more coherently to meet their needs. In local Children's Centres, a similarly diverse range of professionals already cooperate to varying degrees to ensure the educational, social and medical needs of vulnerable youngsters are met. It would be advantageous if such practices could become more uniform, based on a more confident understanding of the power to share data.

In short, both service improvement and greater efficiency rely on: (a) identifying those agencies which share large groups of service users, or share responsibility for particular complex cases; and (b) enabling data sharing to take place between them.

Currently, however, data sharing mainly takes place within single agencies or departments, not between them. Where sharing does occur, this is usually through a "statutory gateway". These allow for only certain acts of data sharing – the records which can be shared are identified before-hand. This makes the process particularly restrictive and renders it unable to respond to the ebb and flow of data that occurs in the day-to-day interaction between citizens and departments.

Service users' contact with public services is rarely divided neatly along the lines of individual administrative departments. There is not a Department for Benefits or a Department for Domestic Violence, for example. This mismatch between the day-to-day reality of government operations and the way in which data is divided is the source of huge inefficiencies and

sub-standard service.

Yet the problem suggests its own solution: where particular cross-cutting user groups – such as benefits claimants, or the victims of domestic violence – exist, their cross-cutting nature should be acknowledged. Professionals dealing with their cases should be required to enable the successful completion of the quite different, but complementary, actions of other professionals in different departments – by providing the data to make their tasks possible.

This solution does not imply the wholesale sharing of *all* information across *all* of government. It relies instead on the identification of processes, which take place across several departments, which contribute to the successful handling of individual complex cases. The power to share data should be limited by the boundaries of customer interaction, rather than the boundaries of bureaucratic departments.

Such an arrangement may well reflect how people expect the state to use their data – acting with coherence and transactional memory in those areas which people associate with the delivery of related services. We believe this observation should provide the foundation for a new data-sharing bill. This bill would move us beyond the case-by-case assessment (and/or legislation) currently required, but would not be a general power to share data. This bill would set out the right, or indeed the responsibility, of departments to share data in cases where they can identify a particular customer group who will experience clearly defined benefits from specified information sharing.

Overcoming obstacles to implementation

There are a number of obstacles to such a seemingly common sense approach. First, it requires the identification of overlapping customer groups across government, which could be a major undertaking. Second, it does not deal with the data requirements of non-solicited services such as tax collection and law enforcement.

Defining service clusters, with overlapping responsibility for delivering similar services to the same people, is going to be crucial to efficient data sharing. We need either to establish transparent logical mechanisms for doing this, or to rely on people's perceptions of similar services that they would expect

to be sharing data. Overlapping services could be identified, for example, by insisting on a rigorous business case as a pre-requisite for data sharing. A key part of any business case would be the identification of either savings through rationalised data collection and processing, or benefits to service users through improved decision making and transactional efficiency from the point of view of the service user. Identifying relevant benefits requires the identification of cross-cutting user groups and the related services they interact with, as well as size of the overlapping customer group and the value of the benefit of the service improvement. This is likely to be challenging. Identifying potential savings may be more straightforward, as the identification of overlapping data collection and processing will reveal duplicated effort which can be rationalised.

Criteria for defining sufficient service overlap to enable, or indeed compel, services to pursue data sharing would need to be arranged in advance. These could be based on the extent of user overlap, or on the value of benefits to citizens/efficiency to government. The latter criteria would seem more useful, as constraining data sharing by the numbers of overlapping users, rather than the value of the services delivered, would mean that relatively rare, but very high value services (such as domestic violence investigations) might be overlooked.

Placing the development of a business case at the heart of data-sharing policy is to some extent an extension of standard government practice, but it creates some interesting further problems. The value to citizens of better services is difficult to quantify in monetary terms. This may be especially true with some service improvements generated by new IT investments, where even efficiency gains to government can be difficult to quantify. For example, it is difficult to measure the benefit to local authorities of website visits rather than face-to-face visits. If we assume there is no value in web site visits, then councils have invested hugely in new technology for no benefit. If each visit to a website saves a council on average 25p, compared to the case when all information is gathered in person, then councils have broken even. If average savings are 50p or even £1, then they have earned an impressive return.[7] Unfortunately, there is no agreed way of estimating the value of a visit to a website.

7 Patrick Dunleavy and Simon Bastow, *Is Measuring Public Sector Productivity So Hard? An Application to Local E-government Change.,* (LSE Public Policy Group, 2005.), P. 18.

The problem of lack of quantifiable benefits looms large in data sharing, particularly when a business case is required not only to demonstrate the benefits to citizens of increased government powers, but also to justify new spending on advanced technology. The difficulty of valuing benefits to users leaves the government with three choices:

- Evaluate benefits qualitatively. Where instinct, experience or best practice suggest data sharing will be highly advantageous, invest in it.
- Withhold investments in new technology except for those cases where benefits can be quantified, such as savings due to more efficient data processing.
- Develop new measures of value to capture, for example, the value to customers of time saved by an efficient transaction process.

Obviously the third option is preferable in the long term. There is considerable academic interest in valuing public sector output and the Office of National Statistics is starting to study the problem too.[8] However, this work may take many years to complete, while service improvements are expected now, and efficiency will be key to CSR 2007. It is therefore highly desirable that government increases the resources dedicated to solving this problem as efficient investment really depends on a solution.

The second option is perhaps least acceptable from the point of view of public service reform, as it would direct investments solely towards projects which benefit the government, only indirectly benefiting users – and then only if the government passes back efficiencies in lower taxes or generally better services. In reality, option one has been used to make progress on data sharing, for example between police forces in the wake of the Soham murders. Certainly, the argument for the qualitative assessment of benefits works well with emotive issues such as child protection. We believe it will continue to have a place alongside increasingly rigorous efforts to value benefits, as departments make cases for increased data sharing powers. The key from the point of view of citizens seems to be that there are significant, identifiable benefits available by increasing data sharing powers between relevant clusters of professionals.

8 In 1998 the ONS began measuring public sector output by using numerical indicators such as the number of operations or lessons delivered in a year. This was an improvement on the previous practice of assuming productivity in the public sector is uniform. The Atkinson Review has begun to explore methods of capturing the "quality", i.e. value, rather than just the numbers of the outputs. See http://www.statistics.gov.uk/default.asp

9 This term was suggested by several delegates at the SMF seminar series (Chatham House rules) associated with this project.

Probably we should refer to a "public interest case" rather than a business case, as the qualitative, but rigorous, presentation of potential improvements will be so important to the process. However, building a business case is an established process in government, one that we hope to see expanded to serve democratic as well as technocratic interests in deciding when to share data. Throughout the paper we therefore refer to "business cases" for data sharing, but use it to mean this wider "public interest case".

We recognise that even where these benefits are large they cannot always be quantified. To remain robust, therefore, a clear mechanism for public scrutiny and oversight must be developed for the assessment of business cases. If possible, this process should be located within existing institutions – creating new offices is not the aim of *Transformational Government*. We feel the Information Commissioner's Office (ICO) is probably best placed to adopt such a role: it is independent of government and has the legal power to challenge government initiatives. Developing a balanced score card by which the ICO could assess the benefits and potential risks of data sharing is a priority for further work.

Building business cases could be led by Whitehall, but they may benefit from inviting practitioner and user engagement in identifying the potential information flows which will add most value to customer experience. This is an issue we deal with later in this report.

Finally, the possibility of a survey-based approach investigating public perceptions of departments which should be sharing data may be a useful public engagement tool and point to the most valuable cases for increased data sharing. The concept of the opinion of the "average reasonable person"[9] may be particularly helpful in deciding how far unsolicited services should have access to shared information. For example, most people would probably agree that if taxes are going to be collected, HMRC should have the information to do it efficiently and fairly. When we consider tackling criminal behaviour such as fraud, the well-established principle of proportionality should continue to apply. This is already the case in the National Fraud Initiative, which could provide a model for more high-powered data-matching exercises targeting greater fraud or security threats.

Proposals

Data sharing between agencies should match patterns of citizen interaction with the state.

Government should identify similar services that customers expect to work coherently together, such as transactional services. Between these services practitioners should be able to share case information as they need, without recourse to further legislation.

For particular complex cases such as domestic violence investigations, authorised practitioners should be able to share information with similarly authorised counterparts, even if they are not in similar services, and would not otherwise share information.

Justification for data sharing in clusters of departments and agencies will have to be made according to an analysis of costs and benefits. An improved method of quantifying the benefits of improved convenience to service users is key to such an approach.

The Information Commissioner's Office could be used to provide an objective assessment of the business case for data sharing developed by particular service clusters. They could veto those programmes which do not enhance the citizens' rights to secure and fair processing of their information, or do not really provide benefits to citizens.

The difference between our suggested approach and the current "statutory gateway" is important. A statutory gateway is inflexible, and only allows for pre-arranged sets of data to be shared. Our suggestion allows for the identification of pre-arranged groups of professionals who can then share *any* relevant data, according to professional need and judgement on the ground.

We expect this to work as follows: the government legislates to recognise the need to share data where a suitably robust business case identifies clear benefits for a particular user group, and where sufficient measures to enhance individual rights are built into the system; departments use these new powers to build business cases for data sharing; a regulator assesses these cases against the primary legislation; departments undertake

the work and training to allow their practitioners to make full use of these new powers. How individuals might use enhanced rights is considered in the next chapter.

We believe this will bring government use of information closer to user expectations of the use of their data. The Data Protection Act (DPA) stipulates that data cannot be used for purposes contrary to those for which it was collected – our proposals bring us closer to a situation in which data is collected once for one purpose. The element of public scrutiny in our proposed system has received some question, but we stand by this mechanism as a means of building public engagement with government and public confidence in data sharing. We discuss this further in Chapter Three, considering the role of law and other regulation.

Chapter Two: Technology, privacy and the information society – the demand for privacy

Introduction

Originally, government hoped that data sharing could support privacy and individual rights. This was the stated intention of Cabinet Office policy when data sharing was first seriously discussed in the Performance and Innovation Unit's (PIU) 2002 report *Privacy and Data Sharing*.[10] This remains an admirable aim. Unfortunately, policy and public discourse have not developed along such lines. As Bellamey et al describe, policy has developed as a precarious balancing act between the competing interests of personal privacy and government efficiency.[11] As this is neither desirable, nor sustainable, it is imperative that we are able to recapture the original aspiration of the PIU, otherwise it is unlikely people will support efforts to use data sharing to improve their services.

Understanding more about the demand for privacy may allow us to focus on policies which produce the desired synergy between privacy and data sharing. In the introduction of this report, we considered the emotional tension between privacy and data sharing. Here, however, we consider privacy as a commodity which people can demand or sacrifice, according to their evaluation of the benefits on offer. This is, in fact, how we treat our privacy in interactions with the private sector, where we are regularly warned that data will be retained for various purposes if we consent to transactions. Considering privacy as a commodity which we can trade in transactions with government makes an excellent starting point for considering how the government might engage with the public to transform data sharing and IT from a threat to privacy into an avenue for increased trust. We suggest several options in this chapter which could contribute to this effort: an increased role for the Information Commissioner's Office, individual consent to data sharing, and citizen oversight of government data processing.

10 *Privacy and Data Sharing* (Cabinet Office, 2002).

11 'Joined Up Government and Privacy in the United Kingdom: Managing Tensions between Data Protection and Social Policy. Part 1', *Public Administration,* 2005, pp 111-133.

The privacy problem: introducing the economics of privacy

If we think of privacy as a commodity, people can choose how much privacy to demand in any situation to make them feel happiest with the circumstances. The levels of privacy people choose will depend on how privacy influences the interaction they are making, and how it will influence future interactions. For example, choosing more privacy might mean slower or more expensive transactions, or filling out more forms; but choosing more privacy might also mean that there is less chance of personal information being misused in the future. We see that privacy has both costs and benefits for an individual in any given interaction.

Whether the costs outweigh the benefits of privacy will depend on the circumstances and the individual's preferences. For example, if giving up some privacy will make a transaction 50 percent faster and two percent cheaper, *and* if we trust the other party to guard our data well, then the costs of privacy will be high, and the benefits low, so most people will give up some privacy. If, on the other hand, giving up some privacy will only make transactions ten percent quicker, and we do not trust the other party, then the costs of privacy will be low and the benefits will be large, so most people will demand more privacy. Different people will attach different importance to speed, price and future risks. Thinking about privacy like this suggests the importance of choice in popularising data sharing, a topic we return to later in the chapter. Below we discuss the costs and benefits of privacy in more detail.

Benefits of privacy

Personal data allows others to influence our lives. If this leads to negative outcomes, there will be benefits to increased privacy.

For example, if fraudsters impersonate our identities, they can steal our money or harm our reputation. This is something which the Home Secretary has highlighted recently, stating that the lack of data sharing is 'is exploited by criminals, especially those involved in fraud. This needs to change. I believe that we can do this without infringing data protection legislation or people's rights.'[12] However, the more data government possesses, the more it can constrain individuals' freedom to do as they please.

Any technology that increases the chances of fraud or excessive control will increase the benefits associated with more privacy. For example, biometric identifiers increase the certainty that data being shared is reliable. This increases the value of the data, including to fraudsters and criminals. Biometrics might also make challenging errors or mis-identification more difficult. Theft of biometric information, or mistakes made processing biometric information could be very damaging to an individual. To stop this happening we might reduce the amount of information we allow others to access. Biometric information might therefore *raise* the demand for privacy, and reduce the acceptability of data sharing because it makes giving up information more risky. This is the reverse of its intended purpose (i.e. to make interactions more secure and so allow increased data sharing).

Similarly, data matching increases the amount of information available to both fraudsters and government.[13] Improper access to matched data would allow unwelcome influence over wider areas of an individuals' life, and so would also increase the demand for privacy. Matched data would also allow data mining techniques to be practiced far more extensively than currently. Such a possible use of technology and process increases the benefits of, and therefore the demand for, privacy. This in turn increases opposition to data sharing.

Costs of privacy

However, privacy also has costs. Receiving goods and services requires us to confirm our identity, and possibly to reveal details of reputation or behaviour which allow others to make judgements about how trustworthy we are. We regularly do this, particularly in transactions with financial services firms. Whenever a service is designed that can allow us to benefit from sharing our data with another party, the costs of privacy – the foregone services or savings – will rise.

12 John Reid, *New Powers Against Organised and Financial Crime* (Home Office, 2006), foreword.

13 Data matching refers to linking one set of an individual's records with another set held elsewhere, something we discuss later in the report.

14 Given that the implications for the secondary uses of such information are poorly understood, potential risks are high – so we must assume that the benefits of privacy are very small compared to cashable returns.

15 *Inclusion Through Innovation. Tackling Social Exclusion Through New Technologies.* (Office of the Deputy Prime Minister, 2005), pp. 15-25.

Often individuals price their data very cheaply, very small opportunity costs cause them to give up large amounts of privacy – for example by revealing consumption habits to a retail chain in return for minor discounts on goods.[14] This strongly suggests that privacy is not an absolute, but something people should be allowed to demand or relinquish as opportunity and preferences dictate.

Government provides services of significantly more value to people than consumer loyalty cards. Where data sharing enhances the value of these services, the *costs* rather than the benefits of privacy will rise, and the demand for privacy should diminish. This is evident from a Social Exclusion Unit report, which found enthusiasm for data sharing to be highest amongst the most vulnerable social groups – government's core service users, who value these services most highly.[15]

As well as increasing the costs of privacy in terms of foregone services, there may be instances in which data sharing can reduce the benefits of privacy. For example, if fewer, shared databases are protected more securely, opportunities for fraud diminish and the benefits of privacy are reduced. This would also diminish the demand for privacy.

Summary

We can therefore characterise potential developments as follows:

- actions/technologies which increase the benefits of privacy
- actions/technologies which increase the costs of privacy
- actions/technologies which reduce the benefits of privacy
- (actions/technologies which reduce the costs of privacy are more difficult to imagine in the context of joining up government).

By concentrating on the eventualities two and three, government could do much to reduce the tensions between data sharing and privacy. *Transformational Government* goes some way towards this. However, is raising awareness of possibilities two and three sufficient to increase public enthusiasm for data

sharing; or does government need to commit to binding agreements *only* to pursue these types of actions? How could government codify such a commitment?

We believe action is required for the government to return to the ground described by the original PIU report, in which data sharing enhances individual rights. In order to do this the government will have to consider the following four questions:

1. Would increased individual choice about the extent of data sharing applied to his or her records enhance citizen's understanding of government data sharing and reduce the demand for privacy?
2. Would increased citizen oversight of government use of data provide foundations for the development of trust between citizens and increasingly extensive data sharing networks?
3. Which practitioners possess the strongest trust relationships with service users, and should data sharing be limited by the prior existence of such trust relationships?
4. Security and government intentions are at the base of potential tensions between data sharing and privacy. Which is the more significant? Can we build solutions that improve our assessment of both?

Practitioners have expressed the hope that placing the citizen at the centre of future data sharing and information policy reforms will help to overcome the tension often registered between efficiency and privacy. This may certainly be the case. Empowering citizens by increasing their access to, and control of, information should improve the trust in, and acceptability of, a system of greater information sharing. At the risk of creating new jargon, the development of the "data subject" into a "data citizen" points the way towards the achievement of initial hopes that data sharing could enhance individual rights.

Choice about the extent to which an individual's records are to be shared could form part of this development, though there has been some scepticism about the operation of consent on a large scale. Nevertheless, allowing the personalisation of data relationships between people and government remains an attractive way of reflecting the heterogeneity of service users.

Often in the private sector consent to data sharing is linked to some financial incentive. Government may wish to explore this, or benefits in kind, especially where returns to citizens are not immediately obvious.

From privacy to trust: public oversight of government data processing

Traditionally, privacy and data sharing have been viewed as opposed alternatives, both desirable, between which we must make the best trade-offs we can. While privacy is undoubtedly valuable in its own right in the absence of interaction, most interactions require us to yield some aspect of our privacy.

In this section we examine the implications of the understanding, drawn from economic theory, that privacy during an interaction is a substitute for *trust,* rather than a desirable commodity in its own right.[16] When government agencies foster trust relationships between service users and professionals, these trust relationships, rather than the assumption of privacy, form the best foundation for governing the use of data.

For example, when we receive goods and services (from a government department, or a bank), we must confirm our identity to validate such transactions. Often we then hand over information which would allow others to pose as ourselves. Such interactions may involve two way risk: when buying a mortgage, we must trust the bank with our identity and financial information, but they must trust us to have provided true financial information and to make good on our obligations. If the bank performs its duties well over time, we may forgive an administrative error, even one that might have been unacceptable at the start of the relationship. Similarly, if we manage our accounts well the bank may improve the terms of our finance, compared to those offered to less well-proven customers. A trust relationship has developed, through the mutual satisfaction of expectations over time, which enables each partner in the transaction to realise additional benefits not possible when the relationship was conducted purely on the basis of legal safeguards prior to the development of trust.

How to establish trust

It is clear, then, that data sharing between citizens and govern-

16 The role and development of trust are much discussed, particularly in the literature of game theory. In the context of data sharing see, for example, Jonathan Cave, *The Economics of Cyber Trust between Cyber Partners,* (Cyber Trust and Crime Prevention Project, 2004).

ment services founded on trust relationships, which emerge as government officials fulfil their obligations to their customers, are of greater benefit to both the citizen and the government. They more likely to yield efficient service delivery and effective decision making than those which operate purely within a legal privacy framework.

In order to establish this trust, as outlined in the bank example above, we must have confidence in the *identity* and in the *intentions* of those with whom we interact.

Confidence in identity.
Securing confidence in identity is relatively simple to address and has a long history in the development of impersonal and remote transactions. The verification of identity is managed by four types of safeguard:

- what you know – biographical history, which is the most widely used
- what you know – shared secrets such as passwords and PIN numbers
- what you have – ID or entitlement cards
- who you are – biometric identifiers (not used currently, except photo ID).

The more sensitive the information involved in an interaction, the more safeguards tend to be combined in a verification process. This is true both in online transactions and in face-to-face transactions between strangers. While no type of safeguard is perfect – all produce false positives/negatives and are vulnerable to fraud – combining several safeguards does reduce these risks. New, strong forms of biometric identification (fingerprints and retina recognition) suggest the possibility of lower error/fraud rates than remote identification systems have previously achieved. But the error rates will never be zero in large populations, whatever technology is used.

Taken to its logical conclusion, improved verification could create a situation in which all government services were accessed via a single combination of identifiers – biometric, token and code – and all data about the citizen was stored centrally, or matched with a common tag such as the National Identity Register Number.[17] In the above situation, the risk of complete identity theft or complete shut out from one's entitlements and accounts will remain, and may grow as fraud catches up with verification technology. This is an important point as such worst-case scenarios are often advanced by opponents of *any* public sector data sharing as an inevitable outcome of moves towards increased data sharing.

17 A number proposed to accompany the National Identity Register in early versions of the ID cards project.

18 A situation of widespread data sharing and low personal and corporate responsibility for security is considered in 'Cyber Trust and Crime Prevention Project. Executive Summary', *Foresight,* June 2004, p20. As this report suggest, any scenario in which data sharing develops too far for the level of security would be an unattractive one.

However, few experts in the field would ever state that a single-verification model is their long-term goal. As we explain in chapter one when we discuss universal versus piece-meal data sharing, efficiency itself imposes limits. To make a case for the efficient and strategic use of data, in support of essential government services, we must reject the over-centralisation, or over-coordination of data, in part because no system of verification and data processing could be sufficiently perfect to support such a powerful potential influence over citizens' lives, even if governments could be trusted to operate in citizens' interests.[18]

Nevertheless, powerful verification systems could increase the public's trust in data handlers being who they claim to be, especially if this is combined with secure data transfer systems which could limit fraud to sufficiently low levels to enable government professionals to share sensitive information about their service users with each other. It is at this more limited scale that improvements in verification seem most immediately useful. Improved verification systems could be useful on both sides of an information transaction: controlling access to terminals operated by data controllers (as GP smart cards do), and verifying the identity of service users (although this is further off, as a general health smart card was recently rejected, partly because of cost considerations).

Confidence in intentions
While technology has the potential to increase our confidence in the *identity* of those with whom we interact, we are still far from a situation in which technology can reveal the *intentions* of those with whom we interact. Developing confidence in someone's intentions remains a matter of repeated interaction, during the course of which we find our expectations about their behaviour fulfilled. It is thus process, not technology, which will determine the ability of citizens to develop trust in government's good

intentions and effective security arrangements.

In many public services, such trust relationships develop as professionals satisfy service users' expectations. The classic example is the health service. OPM research recently identified the NHS as the public service enjoying by far the highest levels of public trust.[19] People have long-term relationships with professionals in the health service, particularly if they use these services regularly. In addition, standards of recruitment and oversight in the health service are particularly high. Reflecting this, the huge majority of treatment is completely satisfactory and people's trust is repeatedly reinforced. When people develop relationships with practitioners in other public services, say a benefits officer or a teacher, they can likewise become confident in the practitioner's intention and ability to act only in their interests. These pre-existing trust relationships could become the foundation for the development of trust in data sharing systems, where such systems are clear extensions of existing professional networks.

A role for consent

Allowing citizens to choose when and how much of their data is shared could also be a valuable method of building on existing trust relationships between individuals and practitioners into general trust relationships between citizens and public service data sharing systems. Consent-based data sharing allows people to make their own evaluations of the services on offer, the practitioners running them and security protecting them. Consent could thus be crucial in winning the trust of the public for further government data sharing. The default assumption of consent-based systems will be an important consideration. We suspect this will ideally vary by service. Very large systems using information which people do not find excessively sensitive will best be pursued with a default opt-in assumption, particularly if efficiencies scale up as uptake rises – transactional services might be an example. However, this will not be acceptable for all systems, as recent developments in the Care Records Service have demonstrated (see Chapter five).

There are two problems with consent though. First, the non-voluntary nature of many interactions with government (e.g. paying taxes) can raise further concerns about the

19 *Research into the Use of Personal Datasets Held by Public Sector Bodies* (Office of Public Management, October 2005).

adaptation of private sector practices to public data sharing. Opposition to voluntary data sharing – tick this box if you want these services to share your data – does exist in some parts of the civil service. Traditionally it has been felt that, because we all pay taxes without choice, we cannot chose what sort of services to expect from government, and certainly not the way these services are administered. We disagree with this argument, and believe that it is based in administrative culture rather than in respect for legal differences between the nature of interaction with the private and the public sectors. It is inconsistent with the development of personalisation and choice, which has been the basis of modern public service reform.

Second, the operation of consent on a large scale has been questioned. If millions of people are changing their consent status daily, interactions will become impossible to manage. In reality it seems unlikely that people will routinely alter their consent status once they make a decision (unless the public sector routinely mishandles their data). However, operating two systems side by side will reduce efficiency savings and possibly create administrative complexity. The costs of operating two systems will have to be carefully considered, because if the government does offer consent-based data sharing, those declining to share must still receive decent (if not improved) services – choice must be real choice.

Beyond consent – oversight

Therefore we may need seek alternative mechanisms for building trust. A third element of building trust is to allow citizens to monitor how their data is being used, and who is accessing it. The Freedom of Information Act (FOI) allows UK citizens to request personal information held about them by government. It also allows citizens to request information about government performance generated by some government processes. FOI has increased citizen oversight of government. But FOI requests are cumbersome and expensive and they were not designed specifically to build trust between citizens and public servants. FOI is therefore a first step in the direction of a just information society, but it is only a first step. With increased government data sharing, we will need a more streamlined, cheap system of oversight; and we will need a system with clear points of citizen

contact and strong processes for sanctioning government officials where citizens uncover abuses. The next paragraphs build on the ideas of FOI and then suggest how to make oversight applicable on a large scale, specifically to promote responsibility and trust in data sharing systems.

First, the system for bringing complaints against and then sanctioning those who abuse positions of trust needs to be made clearer and stronger. We propose that for each customer or service group identified through the process described in Chapter 1, there should be a single point of contact for trust issues. This responsibility could be located either within a lead department in the cluster, or with the customer group commissioners suggested in *Transformational Government.* It is crucial that these offices not only provide information, as under current FOI, but that they have clear powers of investigation and sanction, for dealing with complaints received when users review government use of their information. These offices should have responsibility for ensuring the probity of the data controllers in their group; they should therefore be assessed by the level of complaints against the data controllers in their group, and have responsibility for reducing this.

Second, we need to expand the role of customer oversight. Databases can easily be designed to create audit trails, recording who has accessed the data they hold. For example, the GP smart card is currently intended to hold an audit trail of GP's access to medical records.

Such oversight has been proposed by the DVLA as a potential solution to its business problem: it must pass details on to many third parties; some of these organisations, especially parking companies, do not always have an appropriate claim to a given individual's data, but certainly do have a legitimate claim to similar data held on other individuals. The DVLA cannot establish in advance the legitimacy of each claim, but data subjects are well placed to know if a particular insurance or parking company has a right to their details.

Citizens could therefore play a major role in evaluating the trustworthiness of third parties who use government data, and of the individual data controllers who guard access to this data. To enable such an outcome, access to audit trails would need to be complemented by swift and effective complaints procedures.

Responding to complaints by citizens could create a new workload for departments administering large databases. However, investigating such complaints could prove a particularly efficient means of evaluating and maintaining appropriate levels of security. Further, taking responsibility for developing trust relationships with citizens would seem to be an appropriate course of action for departments wishing to engage in increased data sharing in an environment which is currently subject to excessive fraud.

How citizens might gain access to audit trails will be an interesting subject for debate – little thinking has yet been done in this area. The DVLA have led the way, evaluating the cost of several options for polling random customers about the validity of enquiries made of their data by private companies. While random surveys would allow the DVLA to make some headway against fraudulent claims, they would not enable citizens to routinely check on the integrity of their details. Such survey methods therefore would not be sufficient to develop a culture of responsibility and trust through interaction, which may develop where citizens have automatic rights to oversee the sharing of their data.

If we are to develop such a culture, online access to audit trails will have to be explored, as the administrative costs of such oversight using hard copies or telephone checks, for example, would otherwise be excessive. Even online access will be costly, and creates two further problems: equity of access and security of access.

Equality and security of oversight

Certainly there is a digital divide in Britain. We do not want to create a situation where middle class citizens can protect their details by routinely checking audit trails over their home-based broadband, while less fortunate individuals are left at the mercy of fraudsters or over-intrusive government. We might mitigate this problem by bearing in mind that *any* checking would reduce fraud – oversight, or rather the environment it creates, would be a sort of public good. As a result, the checking carried out by those with easy Internet access will also benefit those without. Further, home based access is not the only way to access internet services: libraries concentrate on providing

access to older and less well off residents and these services are well used, and internet cafes offer cheap online access.

While problems of equality are not an absolute barrier, the problem of security may be much more of a barrier to the development of the routine audit of data controllers by data subjects, or indeed "data citizens". Audit trails record the institutions with which the data subject interacts, creating an outline of their life, yielding a great deal more information to data controllers than any single interaction would. The Information Commissioner takes the view that this is an unacceptable intrusion into privacy.[20] In the light of such cogent opposition, we must consider who has access to audit trails, and how this access is itself recorded. If the audit trail is potentially the most revealing information about a person contained on any database, it will also be the most valuable and the most likely to be targeted by fraudsters and investigators in the business of selling identity information. Access to audit trails may therefore have to be even more closely guarded than access to the ordinary details of a database. Possibly this would require the combination of all three forms of identifier, (knowledge, possession, characteristics), including strong modern biometrics. However, the Estonians offer an alternative solution, based on knowledge of a password and possession of a smartcard to be used on readers on PCs. A log of all transactions is then disseminated to citizens through a national email system.

Such a solution would require the roll out of much new card reading technology to access points across the country. While the roll out of direct debit payment facilities to post offices administering benefits clearly demonstrates that the government is capable of such feats, any future Public Key Infrastructure (PKI) would be an even larger problem. Even then, security would not be perfect. Fortunately, technological guards are not the only weapons we have against criminality: as the Information Commissioner points out, criminal sanctions can be used to make such forms of fraud far less attractive than they currently are.[21] Certainly harsh penalties could be introduced for people abusing such powerful tools as audit trails. Could this reduce abuse to an extent where the benefits of data sharing offset these risks?

20 http://www.ico.gov.uk/about_us/news_and_views/current_topics/identity_cards.aspx

21 *What Price Privacy. The unlawful trade in confidential personal information* (ICO, May 2006).

22 However, Estonia has a population the size of a moderate English town. While we can borrow good ideas from Estonia, we cannot assume that government here should be as technologically driven as the Estonian government – complexity and risk in technology displays increasing returns to scale.

Proposals

Interactions based on trust can be far more rewarding than those based on purely legal privacy rights. However, to improve trust, the government must encourage confidence in the identity and intentions of its public servants amongst the public. There are a variety of ways in which it might be able to build upon existing public trust in public servants, such as GPs and teachers.

First, people could be given a choice about whether particular services may share their data. Their consent can be expressly given or withheld in interactions with different service clusters, depending on how citizens view the potential costs and benefits of data sharing between different parts of government.

Second, we should continue to build on the FOI framework by designating a single point of contact within each customer/service cluster to deal with complaints about data use. This responsibility could lie within a lead department, or with the customer group commissioners proposed in *Transformational Government.* The responsible party should have clear powers of investigation and censure, including bringing harsher criminal penalties against public servants who deliberately misuse data.

Third, citizens could be granted access to audit trails generated on their records, so that they can monitor government and third party activity. Cost implications of the associated technology may make this a long-term solution only. (See below)

An illustration of how to establish trust – ID cards in other countries

Few countries have very successful ID card systems. ID cards require a significant amount of trust between citizen and government. However, where systems *have* been successful, it seems a clear purpose and demand for the card has been recognised, followed by a design which maximises citizen benefits. It is in this way that trust has been established.

Estonia has an excellent solution for national electronic ID cards.[22] The public information contained on Estonian ID cards can be held openly because of well-developed security proce-

dures around the PKI, but also because the information held on the card is considered public information. However, its success is largely due to how useful it is to Estonians, underpinned by a high degree of Internet penetration and on-line interaction with the government. For example, 78% of Estonians filed tax returns on-line in 2004, compared with 17% of Britons.[23] The card is increasingly being used in other service areas, such as travel. The development of secure on-line authentication in Estonia has provided a significant improvement in the quality of well-used services, leading to high uptake of the ID card and increased on-line transactions, and classic ICT efficiencies from the substitution of paper processes.

Crucially, the national ID card has been developed precisely to support the uptake of online interactions. By contrast, it is not certain what problem the British ID card was developed to solve.

Looking further at the Estonian ID card, we can see why it has avoided much of the unpopularity surrounding the British effort. Sensitive information is not held on the Estonian ID card, but in institutions' databases. (Actually, very little sensitive information will be held on the British version either). The card acts as a key, giving citizens access to their data and allowing them to authenticate their identity. Authentication is provided by two electronic certificates, which confirm the holder's name and ID number; these certificates are protected by pin numbers. The system is further protected by a national email address which forwards a record of all transactions to specified user accounts. This feedback is important: it allows citizens to monitor the security of their accounts. Of course, no system is perfectly secure; undetected fraud could occur if someone hacked the secure national email system and changed people's forwarding addresses. However, complete security is never the aim – the aim is to provide sufficient security that overall people experience far more service efficiencies than they experience inefficiencies due to crime.

The Finnish experience with ID cards illustrates what happens when benefits are not clearly linked to their introduction. Although the government developed a technically successful system, uptake has been disappointing and most government services do not use it for authentication. The OECD suggest

23 For UK see Comptroller and Auditor General HM Revenue & Customs, *Filing of Income Tax Self-assessment Returns* (National Audit Office, June 2005) p. 14. For Estonia see http://www.iimahd.ernet.in/egov/ifip/nov2005/article7.htm

24 *E-government in Finland: An Assessment* (OECD policy brief, 2003), p.3.

that Finland have in fact run too far ahead in developing new services, and that "technical solutions should follow rather than anticipate demand for services."[24] The technical barrier here is not so much an ability to come up with innovative solutions – but knowing when demand for services will justify the investment in their development.

Lessons for the UK

Encouragingly, the UK ID card is not so far removed from successful models as it may appear given its coverage. But there are two key exceptions to this: some sensitive biometric information will be stored on the card, albeit encrypted; a central database of transactions made on ID cards will be created in the Home Office. We feel this leads to the following lessons:

1) In order to establish sufficient trust around a new ID card, it must be designed around what the public want and need (either in terms of transactions or security), rather than what technology is potentially capable of. This may mean an ID card is not yet required.
2) The UK should design an ID card with clear benefits for citizens, rather than unclear benefits for government. The benefits of the new solution must then be marketed consistently, for long enough to change established opinion.
3) The card should be a key to access records held in institutional databases, and not create a new central database as a target for fraud. The citizen, not the government, should own the trail of transactions created by the ID card.
4) ID cards should not invite fraudsters to compromise biometric information. Enhanced security should be achieved by ensuring the card generates an instant record of transactions and transmits this record to the cardholder, not to the government.

The implications of these lessons are first: if the government is to press ahead with an ID card scheme based around benefits to citizens, it must create a programme of work designed to enable online and routine transactions with all its services, in order to make the ID card a tool of convenience. No further steps should be taken towards implementation of ID cards until suit-

able transaction technology is in place in the public and private sector. Alternatively, a clear case for the security benefits of ID cards should be made. Only in such circumstances can there be a robust cost-benefit case for investment in the technology required to use identity cards across a range of services.

Second, enlisting individuals in policing their own information may provide better results than highly developed biometrics. Increasing the number of different safeguards will be at least as important to improving ID security as increasing the accuracy and complexity of information about physical identity.

Third, the government have already suggested creating an audit trail of transactions on any national ID card. Unfortunately they do not intend to use this to improve security, but rather to create a central database to hold this information. We would suggest that citizens not government should possess the record of transactions generated by their ID cards. If government needs to know a particular individual's transaction history – say for national security purposes – they should have to apply for the digital equivalent of a search warrant in order to obtain access. We believe the principle of proportionality should apply to searching citizens' information as much as it applies to searching citizens' houses. This is how progress has been made – for example by the Audit Commission – in tackling fraud, we believe proportionality should continue to inform the use of data to tackle fraud, and also to fight terrorism.

Chapter Three: Barrier or safeguard – the legal framework and cross-departmental data sharing.[25]

Introduction

The relationship between law and data sharing will be a major feature of the upcoming public debate about the government's new information policy. Much of this debate is misleading and we try to correct some common misinterpretations below.

In this chapter we consider what the role of law should be in safeguarding privacy, and consider how our proposal for increased data sharing between specific parts of government will fit in with the legal framework.

Protecting privacy: public oversight or legal complexity?

Law has an important role in protecting our privacy. Two areas of law are commonly referred to as "privacy law": the Human Rights Act (HRA) and the Data Protection Act (DPA). The HRA guarantees the right to a private life; however, the act also lists a series of reasons for which reasonable democratic governments may share information, with or without consent. The DPA stipulates that data should be obtained for one or more stated purposes, and not further processed in any manner incompatible with those purposes; but it does not stipulate, or even suggest, that the purposes of one department are necessarily incompatible with the purposes of another.

It is clear that the HRA and the DPA are there to protect citizens from abuse by overbearing governments (or overbear-

25 The SMF is not a legal institution, and this is not legal guidance. The following is based on guidance from the Department of Constitutional Affairs, evidence of other departments' interpretations of the legal framework for data sharing, public inquiries and Cabinet Office outputs. We discuss the legal framework, as presented by the DCA in *Public Sector Data Sharing: Guidance on the Law* (DCA, November 2003), which was the most up-to-date available at the time. We concentrate on the policy implications of the legal issues presented by the DCA, and suggest potential interpretations of the law, which would follow from a logical policy-making brief, though we accept there may be further legal complications we have not considered in these initial thoughts.

ing citizens). This is right and proper. It is also clear that the DPA and HRA are not designed to maintain the current status-quo around information sharing, and make no assumption that the current state of play is the optimal solution. They are there to guard against abuse, not to prevent democratic societies developing coherent, efficient information policies. We therefore feel that neither the DPA nor the HRA would be contravened by the proposal in chapter one which states that data sharing be enabled where the benefits outweigh any risks identified in a publicly accountable assessment process.

However, often the guidance issued to public servants concerning these areas of law is so thorough, complex and impenetrable that it precludes any data sharing. Public servants become intimidated by the clauses and caveats included in the guidance and therefore err on the side of caution when dealing with anything which may come under the auspices of the DPA and HRA. We do not feel that this reflects the purpose of these laws – to protect people from abuse. As the Soham murders so tragically demonstrated, overcautious interpretation of these acts can in fact enable the most terrible abuses of individual rights. Simplified legal guidance, combined with the increased public scrutiny proposed earlier in this report, will provide much better regulation of information use than merely stifling all data sharing by the complex presentation of privacy laws. As part of this process, the central departments and their agencies could consider developing roles similar to the "Caldicott Guardians" who oversee data sharing in the NHS and social services. This possibility exists in current legislation, but has not really been taken up. This would free the ICO from providing routine guidance, leaving scope for other duties. At the end of the chapter we discuss the role of the ICO counterpart in France, where the office plays a major role in endorsing or rejecting potential data sharing projects based on an assessment of their risks *and benefits* to citizens.

Cross-departmental data sharing and the law

The British legal framework is highly complex, with five overlapping areas of law regulating the possibility of data sharing. This includes the DPA and the HRA, but also the law of confidentiality, administrative law, and the European Convention on Human Rights. How will our proposals fit in with laws?

For our purposes, there is no real difference between the HRA and the European Convention, which was its forebear and inspiration. We have already suggested that the DPA and HRA will not prevent sensible data sharing. The real problem is administrative law, and this will have to be confronted if the government is to make progress on *Transformational Government* and the joining up agenda.

Administrative law defines the powers of government departments. All departments must have powers to undertake any action they do: no public servant may do anything *ultra vires,* outside the powers granted to their department so it can carry out its public functions. This is a key limitation on the power government, which is proper to maintain: data sharing should be about better government, not more powerful government.

However, administrative law does present a problem to cross-departmental sharing because each government department is a separate legal entity under administrative law – specific responsibilities and powers are granted to specific departments, not to government as a whole. This means (in our understanding) that both the department giving out data and the department receiving data must have powers to undertake the actions for which the sharing is being pursued. For example, to give HMRC information for the purpose of administering tax credits, DWP would need to have powers to administer tax credits – which it does not. This prevents any data sharing. The astute reader will notice that the fact a tax credit is a benefit with a politically convenient name, and that DWP does have power to administer benefits, is not taken into account.[26] Departments *may* be able to use implied powers to get round such problems, but most public servants agree with our interpretation that they cannot.[27]

Nevertheless, departments clearly need to have the powers to undertake sensible acts of data sharing. Data sharing is a specific action which impacts on the possibility of another department doing its job. The nature of data sharing (and the withholding of data) should be acknowledged by administrative law as a specific action that influences the possibility of other parts of government carrying out their statutory duties. Therefore,

26 In this case DWP could actually use a statutory gateway to get over the problem, and it does; but this can create more difficulty than it removes and is discussed further below.

27 See *New powers Against Organised and Financial Crime,* op. cit, in which the Home Office takes our view.

departments should be given the power to share data for the purpose of enabling other departments to carry out their duties. Again, we would expect these powers to be granted only where clear customer benefits have been identified, as we explain in chapter one.

It is crucial to recognise that we are not suggesting departments start carrying out each other's duties. Some in the privacy lobby feel that to enable any data sharing, the government would have to compromise the legal separation of departments and government bodies would start acting as one – doctors would start asking people for their taxes and policemen would be offering social care. This fear takes little account of the nature of different institutional priorities and is highly unlikely in any circumstances. Nevertheless, it is important to emphasise that giving a department the power to *enable* another to carry out its duties is not the same as giving one department the power to carry out another's duties. In this approach, the legal separation of powers would remain, but the cross-cutting nature of information would be acknowledged.

Proposals

Administrative law must establish the power of departments to share data to enable another department to discharge its duties. These powers should reflect the identification of cross cutting user groups, suggested in chapter one.

DPA guidelines should be revised to emphasise the possibility of data sharing between practitioners contributing to a clearly identified, justified purpose.

Central departments and their agencies should develop roles similar to the "Caldicott Guardians" who oversee data sharing in the NHS and social services. This possibility exists in current legislation, but has not really been taken up. This would free the ICO from providing routine guidance, leaving scope for other duties.

A further role for the ICO could be developed from the French model; this would allow the ICO to assess the benefits of service improvements against potential risks to privacy, rather than just assess legal compliance. ICO powers to block projects could be increased to ensure its continued independence.

28 *Public Sector Data Sharing: Guidance on the Law*, op. cit. introduction.

29 ibid.

The remainder of this chapter discusses the legal framework (including confidentiality) in much more detail, and develops our arguments more thoroughly. We then consider international evidence on legal frameworks and suggest how best the government could approach the implementation of our proposals. This should be read only as a companion to the main arguments above, for those who want to interrogate the evidence more thoroughly.

Overview of British law

There are five areas of law which regulate the possibility of public sector data sharing:

- administrative law
- common law and statutory obligations of confidentiality
- European Convention on Human Rights
- The Human Rights Act (we treat 3 & 4 together below)
- The Data Protection Act (DPA)

Individually, none of these regulations prevents the development of a strategic rather than a bureaucratic approach to the use of public sector data. Together, however, they create a framework which the Department of Constitutional Affairs (DCA) would agree "is generally recognised [to be] complex".[28] This complexity does present a difficulty for officials and policy makers trying to identify data sharing solutions to service delivery problems. Discussing the five relevant areas of law in turn will allow us to separate out some of the opportunities and problems – often more political or interpretive than purely legal – which arise from the current framework.

Our discussion will generally concentrate on possibilities that arise *within* the existing framework, which we assume will largely remain intact to regulate future data sharing initiatives. As the DCA point out "the law rightly puts in place safeguards for the use of individuals' data."[29]

It is often noted that the private sector engages in quite widespread data collection and sharing, across organisational

boundaries, without contravening the law. However, administrative law does not apply to the private sector. Administrative law imposes restrictions on the powers of public bodies to undertake actions in pursuit of their aims. This problem, the key legal barrier, is discussed first.

First we review the British legal framework, before looking at international efforts to overcome legal barriers to data sharing, and suggesting a way forward

Administrative law: do departments, agencies and officials have the authority to share data?

Administrative law, rather than the DPA, is certainly the most fundamental, and probably the most problematic area of law relating to public sector data sharing. Administrative law governs the actions of public bodies, including the Crown Ministries and Statutory Departments that are the focus of this study. A key principle of administrative law is that such bodies may never do anything that is *ultra vires,* outside the powers they are specifically granted to carry out their statutory duties. Each department is a separate legal personality and only possesses powers to facilitate those actions that constitute its particular statutory remit.

There is no statutory power to collect, keep or process data. Data sharing (an act of processing) can only be considered if it facilitates some statutory action. Departments sharing and obtaining data must *both* have the authority to carry out the function for which the data is being processed. Given the division of responsibilities between legally separate government departments, the existence of powers to share data can therefore be difficult to establish.

This has led to the development of "statutory gateways" as a vehicle for data sharing. A gateway is a specific piece of legislation enabling, indeed requiring, specific data to be exchanged between two parties. In general, the DWP uses such mechanisms for obtaining and sharing data with other departments. However, such gateways can create more difficulties than they resolve due to their inflexible nature. While statutory gateways can enable tightly defined data sharing operations, they are not always suitable for catering to individual citizen's experience of government and the data required for each individual's variety

30 For example,http://www.theregister.co.uk/2006/03/30/public_service_transformation_underway/

of transactions – for example, they cannot easily cover for the ebb and flow of relevant information about, say, the service needs of a vulnerable child. Gateways also tend to reduce non-specified data exchange, and so in fact may do more harm than good in cases of cross cutting requirements.

It seems that the recognition of cross cutting customer groups, which always underpin the 'joining-up' agenda and has been recognised by the Service Transformation Board,[30] is evidence that the statutory responsibilities of individual government departments are complementary actions; actions that can only be successfully completed in concert and not in isolation. However, this understanding has run ahead of existing interpretations of the legal foundations of government action.

The limitation of powers imposed on public bodies by administrative law is a crucial safeguard in our constitutional system, one that must remain. Likewise the legal separation of government departments is certainly necessary. Nevertheless, the fact remains that, whether protecting vulnerable people or delivering benefits a range of government departments must interact with any given person; people have the right to expect those departments to act constructively and coherently to meet their needs. Such recognition may require a reinterpretation of the *vires* granted to public bodies in pursuit of their complementary agendas. Where departments view only their specific contribution to such a process as being *intra vires,* it can create a proprietary "data-silo" environment, that limits the ability of professionals to make fully informed decisions.

If government is to use technology to really become joined up, it must have the powers to act in a joined up way where appropriate. Currently this is not the case due to the separation of powers along administrative lines.

Common and statutory law of confidentiality

Obligations of confidence are incurred when practitioners record and process "sensitive" information about an individual. Practitioners controlling such information have a legal duty not to disclose this information to third parties. The Common Law Tort of confidence provides people with a route to damages when this duty is breached. Currently the legal separation of government departments means that information transferred

between them is subject to this law. Most information that government deals with – including names and addresses – can potentially be considered "sensitive".

However, the law of confidentiality ceases to apply if people give authorisation for their data to be shared, as would be the case if increased data sharing were to be pursued through individual consent (a prospect we suggest above). The law of confidentiality also ceases to apply where data controllers face legal duties to disclose information. Politicians could choose to make such disclosure routine between similar services, such as the transactional services (the DWP and HMRC), where the public would expect such data sharing, or where the benefits would be large.

Human rights legislation

Though enacted in two parts, these areas of law can be, for our limited purposes, discussed together. The key part of human rights law bearing on data sharing is Article 8 of the European Convention on Human Rights.

> Article 8. Everyone has the right to respect for his private and family life, his home and his correspondence.

The information covered by Article 8 includes all personal information so, for example, passing on names and addresses to private companies would constitute a violation of the right to privacy, and would not be an acceptable form of public sector data sharing. However, data sharing can be pursued in the public interest, despite Article 8. Based on DCA guidance, there are circumstances in which the state can override individual rights to privacy. Any action that overrides the right to privacy, described in Article 8, must be:

- "in accordance with the law",
- serve a "legitimate aim", and be
- "necessary in a democratic society".

The "legitimate aims" described above are then further defined as:

- upholding national security
- upholding public safety
- ensuring the economic well-being of the country
- preventing disorder and crime
- protecting health
- protecting morals
- protecting the rights and freedoms of others.[31]

31 *Public Sector Data Sharing: Guidance on the Law*, op. cit.

The list of legitimate aims is sufficient to cover most of the reasons for which a government may wish to share data. For example, data sharing to administer benefits is necessary to the economic well-being of the country, while broader action against fraud might fall into this category as well as into the prevention of crime. The last category – protection of the rights and freedoms of others – is particularly broad, and could feasibly include controversial measures, such as police access to health records, which are likely to be disputed at practitioner level before the government runs into legal difficulties.

The DCA, therefore, suggests that the most difficult test will be that of "necessity in a democratic society" in Article 8. The satisfaction of this test will turn on the interpretation of necessity; necessity is, in turn, believed to rest on an assessment of "proportionality" in the use of power to achieve a "sufficiently well defined" legitimate aim (from the list above).

Case law so far suggests that, in assessing proportionality, courts will have to consider the "balance" struck between the right to privacy and the aim pursued through data sharing. Privacy and sharing are assumed to be in tension. The court must assess whether the interests of privacy and of public good have each received appropriate "relative weight" in the decision to share data. Satisfying this test requires sufficient safeguards to be placed around the further processing of personal information in its new institutional context. Satisfying proportionality therefore demands that only those who need to see the shared data have access to it. This restriction must be supported by effective criminal and civil sanctions. This goes beyond the test used before the Human Rights Act, in which the court merely required a greater justification for a greater intrusion into privacy. This would not therefore be a barrier to data sharing between relevant practitioners to deliver benefits to

service users.

This permissiveness has been demonstrated by European case law. The ability of the state to demand private data – including health records – for the administration of benefits, the completion of censuses and the administration of taxation have all been upheld by the European Court of Human Rights, where the above safeguards have been met. Distributing the resources of the public purse effectively is thus shown to be one of the chief interpretations of the "economic well-being" of the country. Data sharing which pursues efficiency or anti-fraud initiatives, or improves the quality of services, is unlikely to fall foul of the Human Rights Act and associated legislation.

The Data Protection Act

The DPA is itself a complex piece of legislation. This is reflected in much departmental guidance on data sharing. Such documents generally begin by warning that data sharing without due cause can result in dismissal and prosecution.[32] While this may not put off fraudsters who accept the risks, it is intimidating for well-meaning staff. Typically, guidance is long and complicated, emphasising the need for bespoke assessment of the trade offs between public interest and individual privacy to accompany every consideration of data sharing.

Data sharing is already a technically and administratively difficult action, as we explain above. As such, circumspect legal advice of the type held in the DPA may provide a dignified reason for departments to refuse to engage in data sharing processes with others. As such, it may be the interpretation of the DPA, rather than the Act itself, which proves an obstacle to data sharing. For example, the Bichard Inquiry found that the DPA has been used as a rationale for the excessively limited use of police data, with disastrous consequences for public safety.[33] The report suggested that it was the administrative interpretation of the Act, rather than its content, that was responsible for the insufficient data processing by the police which in part allowed the Soham child murders to occur.

Following the enquiry, and further demonstrating the actual flexibility of the DPA, forces which had previously been destroying data in the name of the DPA cooperated to begin the establishment of a new Code of Practice on information sharing, with no change whatsoever in the legal framework.[34] The DCA has also emphasised the actually quite permissive nature of the DPA. For example, the Act requires the sharing of data to be "necessary". The DCA provides explicit guidance that "necessary" should be taken to mean "reasonably required, or legally ancillary to" the function concerned. Interpretation of "necessary" is specifically *not* limited to actions which are "absolutely essential" to the carrying out of public purposes, and could therefore include actions which allow these processes to be done more satisfactorily, rather than just those actions necessary for a bare minimum of service provision. The DCA point to the administrative court's refusal to rule that police publication of offenders' names and photographs was a breach of the DPA as such an example. In this case, the court was not convinced that the information sharing – the publication of name and photo – were not a proportionate response to the discharge of police obligations to reduce crime and disorder.[35]

Thus, where cross-cutting user groups and departmentally divided processes are identified, the DPA should not prove an obstacle to the strategic use of data to support these common purposes, if used correctly. In fact, many actions of sharing which are problematic from the point of view of administrative law would *not* be a problem from the point of view of the DPA: while administrative law demands that both those who acquire and share data have the *vires* to carry out the act for which the sharing is undertaken, the DPA only insists that the actions of both parties serve a sufficiently defined public purpose. If cross-departmental data sharing can be reconciled with administrative law, the DPA is unlikely to prove a further barrier.

Thus, a key question for future data sharing policy will be how to translate a permissive interpretation of the DPA into suitably permissive data sharing guidance for those professionals who most require data sharing to deliver increasingly demanding personalisation and service delivery targets. Will such guidance be centrally imposed, or will it arise naturally, where central departments are persuaded of the business case for a data sharing initiative?

32 *Data Sharing and Data Matching of Personal Information,* (Department for Work and Pensions, December 2004), p. 1.

33 *The Bichard Inquiry Report* (Home Office, 2004), pp 3-4.

34 ibid. p. 14.

35 *Public Sector Data Sharing: Guidance on the Law,* op.cit.

Summary

There are two problems for government:

- the absence of powers for cross-departmental data sharing
- existing constrictive interpretations of the DPA, which must be overcome.

We now review international evidence on government approaches to data sharing and the law, and conclude by offering some suggestions for the way forward in the UK.

How can the government review the law and change cultures of legal interpretation?

International evidence

There is a clear difference between e-government policy in Scandinavian countries and the rest of the world. Scandinavian governments enjoy such a degree of trust that they are actively able to review privacy legislation and pass laws which enable data sharing, while protecting citizens' rights.

The problem facing governments whose citizens are more sceptical and more private than the Scandinavians, is to update legal regulations without alienating their citizens and creating further barriers to the up-take of online services. Australia has similar problems to the UK in this respect while Estonia, often hailed as an example of best practice, has also fallen foul of regulatory complication. Mexican administrators report greater difficulty negotiating internal contract and management regulations than negotiating the law, but this is an easier problem for governments to solve. France offers an interesting example of combining legal regulation with the pursuit of openness.

Estonia demonstrates problems that can arise if governments fail to address the legal and regulatory environment before pioneering technical solutions. Estonia's data control legislation is considerably less flexible than our own. This has led to frustrating delays in the uptake of data sharing services provided through *X-road*.[36] X-road is an excellent technical solution, which allows databases from across government to be linked, via secure Internet connections, to any citizens or civil servants participating in the scheme. Unfortunately, Estonian law bans the "cross usage of data" and the simultaneous processing of

36 See below

data from different databases.[37] Agencies wishing to link their databases to the interface were delayed as the technical solution had run ahead of Estonia's legal framework. This interrupted agency plans and high expectations were let down.

37 'Gaps in the Legislation' http://www.riso.ee/en/pub/2002it/p22_t.htm

The Estonians believe similar laws do not exist in the West. It is certainly true that our Attorney General recommends a liberal interpretation of the 'single use of data' clause in the Data Protection Act. Nevertheless, this hitch indicates the need to ensure that interpretation of laws, such as the use of data for a single purpose, is agreed across different administrative bodies.

A further problem for Estonia is the absence of legislation covering the use of public data by private companies. Businesses were initially intended to benefit from Estonia's data sharing system, but without such legislation they cannot participate. The Home Office has suggested corporate uses for a national identity register, so it is not yet clear whether similar problems may occur in Britain. Estonian experience clearly demonstrates that technical solutions need to be compatible with legal and regulatory frameworks, or they will not deliver planned benefits.

38 *OECD E-Government Studies: Norway Assessment* (OECD, 2004), p. 3.

The Scandinavian nations suggest one possible course for activist governments:

In Norway the government has legislated on privacy and electronic communication with the express purpose of overcoming legal and regulatory barriers to e-government, particularly the provision of on-line services. Norway has a tradition of "rigour in legislative simplification", which Britain probably does not.[38] As a result, the working groups charged with designing a new legal framework, to enable progress in crucial policy areas such as Public Key Infrastructure (PKI), did not arouse widespread popular opposition. These working groups, including elected and non-elected public servants, were not seen as a threat to individuals' rights, as they might be in Britain.

The Swedish government also takes an active role in reviewing legislation, and amending it to enable democratically agreed public service priorities. The government enjoys a high degree of trust, particularly in the area of information handling, where there is a strong tradition of individual rights legislation. Indeed Sweden pioneered Freedom of Information (FOI), with a Freedom of the Press Act, 1766, which remained in operation

to 1949, giving citizens rights similar to our new FOI rights.[39] This transparency has given Swedish governments far more credibility than their British counterparts.

Finland likewise enjoys coherent, recent legislation – pioneered by the Ministry of Justice – designed to enable advanced e-government. The laws cover electronic identification, data exchange and authentication. There is good guidance on technical standards, though some agencies reported to the OECD that further regulations are "fragmented" and this has led to delay in implementing the e-government strategy.[40] Such developments at least demonstrate that the legal and regulatory framework need not be perfect for the successful pursuit of higher-functioning online services. (Finland scores well in e-government surveys despite these problems).

While such faith in government could develop in the UK, FOI has been only one of a number of new policies deemed to impact on citizens' rights versus the state. Other policies, such as the anti-terror laws, seem to strengthen the state against the individual. Attitudes to these developments could easily spill over and shape people's opinions of any government efforts to review the regulatory framework governing data sharing.

France may offer some guidance on how to achieve transparency and regulatory rigour while promoting an environment for e-government. France has strong regulations regarding the use of new technology to share data. New technology, however, is being embraced, with the ultimate aim of creating a system of personalised citizen portals, through which citizens can access information and services. This will reduce the number of contacts required to administer services, and improve the information available to civil servants in the exercise of their duties. The strong regulatory structure is intended to secure public support for this data sharing process. By law, all ministries or agencies intending to pursue a data sharing initiative must declare the project to the *Commission Nationale de l'Informatique et des Libertes* (CNIL) which assesses the project in terms of the transparency and ease with which individuals' can effect their rights under Council of Europe Convention 108 (enshrined, in the UK, in the Data Protection Act). Public bodies must supply *CNIL* with details of the aim of the project, the data recorded to pursue this aim, how long the data will be stored, and who the persons having access will be.

39 *E-Government in the member states of the European Union* (IDABC, 2005), p. 513.

40 *E-Government in Finland: An Assessment* (OECD policy brief, 2003), p. 3.

French law thus contains a clear process by which government data sharing projects are made public and assessed in terms of individual rights. Though stringent, the clarity of the regulatory process, both in terms of compliance and public scrutiny, makes it an avenue of progress rather than an impediment to data sharing.

Summary

The Norwegian example suggests that a specialist cross-government body could be useful – Misc. 31 could perform such a role. The Scandinavian tradition of continual regulatory renewal also suggests the Better Regulation Task Force could have ongoing responsibility for regulations governing the use of information and its associated technology. Certainly the French example of making regulations simple but stringent, and public, but easy to comply with, seems more efficient than our own reliance on multiple overlapping areas of law, combined with limited powers of scrutiny for the public.

Overall, there is strong evidence that legal renewal is possible, necessary and positive. Public acceptability will be key to the success of the initiative – this will require openness and commitment to user, rather than government benefits. The ICO could have a role in this, as we suggest in chapter five.

Could this happen in the UK?

There have already been significant changes in data sharing culture in the UK. The Bichard Inquiry followed a series of events that demonstrated the dangers of legal complexity providing an excuse to avoid service improvements through increased data sharing. In fact, neither the Data Protection Act nor the Human Rights Act would have prevented sharing data in this instance.

Experts in this field have noted that the legal situation around data sharing has become more conducive for many activities in recent years, following the Victoria Climbie tragedy, the Bichard Inquiry and a greater determination to combat fraud as outlined recently by the *New Powers Against Organised and Financial Crime*. There is a general feeling that the Data Protection Act and the Human Rights Act would not pose a major barrier to carefully planned data sharing, delivering real

benefits to citizens.

We therefore feel that if legal review is pursued as part of a citizen-centred information strategy, this will not raise problems of privacy.

The government does not have an outstanding reputation for either overseeing large IT projects, or protecting individuals' rights in a coherent manner. The government will therefore have to think particularly carefully about public consultation and transparency when reviewing the law governing privacy. Expanding the role of the Information Commissioner and graduating from a situation of arcane legal safeguard to safeguards based on public scrutiny and oversight could be crucial to the success of such efforts.

Section Two: Practical and Technical Challenges

We have looked at some of the broad problems facing the government as it considers an information policy for the 21st Century.

In the following chapters, we consider

- how the effort to join up information flows will impact on other government structures such as budgets and Public Service Agreements
- how cross-departmental IT projects can be managed – should they be led nationally or locally?
- how to ensure successful relationships between departments cooperating to a greater extent than ever before, including
  – data matching
  – agreeing common terms
  – the free rider problem, contracts and compensation for effort.

In chapter four we see that the effort to join up information flows between appropriate parts of government will requiring further joining up of administrative structures if it is to be successful. Chapter five considers whether the government stands much chance of success in managing further IT investments. A strong learning process is identified in progress so far, and combined with international experience it suggests that the emerging aspiration towards centrally defined standards and local control over implementation is very encouraging. We then consider how this attractive combination can be realised in practice. In the final chapter we explore the organisation of new data sharing projects – what preliminary work must be undertaken, and

how can effective relationships be built and maintained when some departments will be saving money and others spending more.

This section may seem more relevant to those few large data sharing projects – concerning say transactions, fraud and security – that require significant IT investment, than to data sharing in general. While this is true, some of the observations about data governance and co-operative working will also be relevant in the more low tech environments where much data sharing, particularly to tackle social exclusion, will take place.

Chapter Four: Joining up government – budgets and interdepartmental cooperation

Introduction

Identifying the need to share data, and building a public case for data sharing powers is a good first step. However, it does not guarantee that departments will have the means to invest in data sharing. In fact, without significant changes to funding and assessment structures, there would be no reason for departments to consider building cases for data sharing in the first place. If new powers to share data are to mean anything, then the elements of funding and assessment that relate to data sharing will have to evolve to support these powers. At the moment the wider structure of government enforces the very data silo environment that impairs public safety, enables fraud and encourages waste.

Increased data sharing will challenge government funding structures from three directions: IT investments are generally hard to manage; government funding and evaluation structures are set up to mirror the administrative divisions which data sharing is supposed to overcome; and data sharing is about changing business processes as well as IT hardware – investing in people is a long term cost that can exceed infrastructure costs. Successful data sharing will therefore require:

- flexible budget mechanisms for handling IT investments
- budgets capable of handling the further change management and staff training costs which increasingly must accompany IT investment

- new funding structures capable of accommodating cross departmental working
- new incentives for cross-departmental working.

There is considerable international evidence on the potential difficulties experienced by governments attempting to improve their IT infrastructure. This is worth reviewing in order to avoid such mistakes in future. Britain has also led the way in committing to large projects, and the experiences of CJIT and CfH again provide useful pointers for future data sharing exercises

International evidence on potential budget difficulties

In Mexico, budgets are often limited and inflexible, and future funds are uncertain. In addition, there is no way of accounting for shared projects. There is a lack of understanding, or use of, e-government business cases. Time horizons tend to be too short for multi-year investments. Nevertheless, many services are online and there is a new e-procurement portal.[41] This demonstrates that early e-government projects have been able to overcome budgetary rigidities and shortfalls; this is because building websites, for example, is relatively simple compared to more advanced developments such as data sharing. The problem for Mexico has been trying to continue progress and develop more complex e-government services without first renewing these essential government processes. Mexican experience clearly suggests that government working practices must be updated to accommodate investment in IT before these investments are made, or the results will be disappointing. While Mexican budgets have been over-centralised and inflexible, Scandinavian heritage is now presenting these countries with the reverse problem.

In line with their decentralised government structures, most Scandinavian countries leave a great deal of budgetary discretion to the operating agencies, at a level below the ministries, which are analogous to our central departments. This budgetary responsibility underpins the strong lower-level leadership and agency innovation that has characterised Scandinavian e-government. However, an increasing focus on cross agency and cross ministry delivery is leading to increasing central direction of funds across the region. While central direction in the service of joined up working is clearly important, Britain could probably also learn much about local institutional buy-in from Scandinavian practices.

41 OECD E-Government Studies: Mexico Assessment (OECD, 2005), p. 2.

42 *OECD E-Government Studies: Finland* (OECD, 2004), p. 10, pp. 42-43.

43 *OECD E-Government Studies: Norway Assessment* (OECD, 2005), p. 3.

In particular, it is worth considering the example of Finland. There many online services were developed with the help of central "one-time funds". The general fiscal environment is tight; the localities spend the money available to them as they choose, but spending decisions are centrally monitored. There is little support for cross-agency funding through these systems. The OECD has recommended that the one-time funds, which helped develop early online services, be used as a template for new innovation funds to support cross-agency projects.[42] Without such funds, further development is unlikely.

Sweden may derive some planning advantage from the fact that the Ministry of Finance holds ultimate responsibility for e-government, placing strategy and financing decisions within the same body. However, many finance ministries would already feel too overburdened to take on e-government responsibility too.

In Norway, central oversight of IT expenditures has also been limited. There has been sufficient money available to local agencies to keep Norway in the middle ranks of online service provision, and ahead in back office applications. The Norwegian Ministry of Finance now exercises more oversight than previously, due to high media coverage of large project failures in the late 1990s. An OECD survey of ministries and agencies indicated "a high level of budgetary barriers with regard to lack of funds and long term and joint funding mechanisms."[43] Norway enjoys a spend forward rule, to enable the highly independent agencies to use some of next year's money on this year's infrastructure spending, but this may not provide sufficient flexibility for all IT projects. However, it may be more a lack of experience with IT business cases, and with collaborative working, than budget limitations per ser that led to the difficulties reported by the Norwegian agencies.

While Britain does avoid most of Mexico's problems, and has been a source of innovation in time flexibility, we do not have mechanisms capable of managing joint investment by cooperating departments. As Scandinavian experience has

demonstrated, this will prevent the development of higher level cross-departmental services. We must overcome this problem to make progress on *Transformational Government*. This will require a major review of Treasury and departmental budget processes. Joint funding must be identified for joint projects, if "joining up government" is to become a reality.

Protecting cross-departmental funding

Returning to the UK, a major obstacle thwarting early efforts to improve the IT infrastructure in health was the absence of ring-fenced IT budgets. The Wanless Report, *Securing our Future Health: Taking a Long Term View,* was set up to examine, amongst other things, the disappointing progress made between 1998 and 2000 on the *Information for Health* strategy. A key finding of the Report was that money earmarked centrally for IT projects was used locally for improvements more immediately obvious to service users. Wanless also found insufficient financial commitment to IT, given the scale of the infrastructure backlog.[44] As a result, both the criminal justice IT system, CJIT, and *Connecting for Health* – Information for Health's successor, now control extremely significant, dedicated budgets – £6 billion in the case of *Connecting for Health,* and £2 billion for CJIT. CJIT and CfH allocate these funds directly. This has led to the transformation of the physical information infrastructure in both services, with the hardware as well as system architecture now in place to allow such essential but previously lacking capability as email communication across these multi-agency services.

This experience points to a potential difficulty in arranging cross-departmental data sharing. Each department's IT unit, being evaluated largely on the functioning of core performances *within* the department, will, like the local general managers before them, face incentives to divert away funds from any new cross-departmental project to support its core functions. If we recognise this as a potential problem though, it is easy to solve: Budgets for cross-departmental initiatives must be clearly earmarked and IT units in both departments must be evaluated on their cooperation and contribution to the joint effort. In later sections of this report, we discuss options for how this effort might be arranged. First, we need to ensure that, where it benefits service users, departments actually make efforts to join up their information processes.

44 Derek Wanless, *Securing our Future Health. Taking a Long Term View* (HM Treasury 2002), p. 101.

Encouraging such cooperation is not only about arranging budgets. Departments which have not contributed to each others performance or worked together before will not start doing so without sufficient incentive. There are essentially two options for creating these incentives, though they may be combined for best effect.

Cooperation can be encouraged by conditional access to additional funding for projects contributing to the 'joining-up' agenda (explained below); alternatively, performance management targets such as Public Service Agreements (PSAs) could be adapted to require cross departmental working where clear benefits have been identified for service users. Combining the two, and using cross-cutting satisfaction surveys, would ensure that actors concerned would have good reason to cooperate to the benefit of service users. For example, a cross departmental team which developed to tender for additional funds and failed would still have an incentive to work together – to meet their PSAs.

Incentives for cross-departmental working: funding

Budget structures could be a key way of creating incentives for departments to share data. This could occur in several ways:

1. Cooperating departments could submit competitive tenders to central government for extra funding dedicated to data sharing projects which will advance the *Transformational* agenda.
2. Departmental budgets could retain ring fenced requirements for cooperative projects.
3. Investment could be undertaken jointly by departments as part of long term planning (with or without additional funding) with costs recouped over time, through more efficient collection and storage of data. Each department would need to know it could make a return on joint investments:
   - this could be arranged by Treasury negotiation
   - it could be arranged by charging departments/agencies to sign up to the system
   - it could be arranged by pricing data flowing within the

information sharing system.

Canada uses central funding actively to support interdepartmental collaboration. The Government on Line (GOL) initiative is intended to develop whole of government solutions, yielding service improvements for citizens, and efficiencies for government through shared infrastructure and improved learning. Individual departments often do not have the funds available to develop investment intensive e-government programmes. However, central funding is available to supplement departmental funds when administrative bodies collaborate to help government meet GOL objectives. Departments put forward their joint projects and bid for funding to implement them. Proposals are assessed against GOL objectives, their technical feasibility and management capacity; and the best proposals receive central funds. Successful multi-departmental projects include: Seniors Canada Online – an information portal for older Canadians; e-Client Application Status – allowing electronic updates on the immigration process; The Canada Site – a huge project to build a single point of entry to all information holdings relevant to interactions between government and its service users. [45] It is possible that Britain's new customer group commissioners could have their own budgets to fund such cross-departmental projects.

Italy has successfully arranged the coordination of three layers of funding – local, regional, central – to overcome limitations in funds that had previously limited the possibility of pursuing the government's vision. A key feature of their success has been the use of tender rather than the normal transfer of funds, allowing the government to select the best projects, increasing accountability and responsibility for project success and encouraging other funding bodies to support chosen programmes.[46]

The US has a strict policy of one project, one agency, one budget funding, in an effort to ensure clear accountability for projects. However, there is a specific exception for e-government projects. The Office of Management and Budget encourages multi agency working through this framework.[47]

45 *OECD E-Government Studies: The E- Government Imperative* (OECD, 2003), p. 58.

46 ibid. p. 59.

47 ibid. p. 60.

48 Such additional funds would not have to be whole-project funds, but would augment departments' ability to 'spend to save', to ensure that whole-project costs, including staff retraining, could be met.

Summary

Common themes in these countries include:

- the coordination of layers of funding
- competitive tendering processes
- and the amalgamation of funds to support fewer, better projects.

These features could usefully be adopted in UK funding mechanisms to support the *Transformational Government* strategy.

One of the reasons why the competitive pursuit of extra funding could be crucial to successful data sharing projects is the relative paucity of tools for evaluating IT investments. We have already discussed the difficulty of valuing outcomes in the context of business cases, and the same difficulties limit the potential of performance management to act effectively and predictably. Evaluation procedures should therefore take a supporting role in fostering cooperation. Changes to budget structures should lead the way.

Assessing which proposals are best placed to deliver value to government customers will require an assessment of the service improvements on offer and the information and technology requirements to realise these. Such a process will require cooperation between the Treasury, which routinely assesses calls for funding, specialists such as the CIO Council, and possibly also the National Audit Office, who have expertise in evaluating the outcomes of previous investment. This would require a specific working party of experts from the above areas of government.

Proposals

Budgets for interdepartmental cooperation should be ring fenced.

Competitive tenders for additional funding would be the best way to organise budgets for information sharing.[48]

Establishing which cases for additional funding would deliver the most value to customers would require an evaluation of the service changes on offer through more sharing, and an assessment of the information and technology requirements to realise them. This would probably require co-operation between the Treasury, which owns the budget process, specialists such as the CIO council and

perhaps the National Audit Office, who specialise in evaluating service outcomes.

Incentives for cross-departmental working: evaluation and performance management

Even with competitive pursuit of additional funding playing a strong part in motivating cooperation, and ensuring only strong projects are funded, there will still be a need for project evaluation and performance management. We now review the international evidence, which largely demonstrates the difficulty of this area, and suggest possible ways forward.

Some UK initiatives may be examples of best practice in this area, notably CJIT's project evaluation procedures.[49] However, not all government IT programmes are so thoroughly assessed. Further difficulties will develop on cross-departmental projects, as most government accountability structures are defined by departmental boundaries.

The OECD suggests the following building blocks for the effective evaluation of e-government initiatives: assessment of the costs, benefits, demand for services provided, and quality of services provided by an e-government investment. However, the difficulty is not identifying this structure, but creating frameworks for the accurate imputation of benefits and assessment of quality which is described. In so far as the OECD advice moves us beyond counting up web pages, it is very welcome. Unfortunately there are few international examples of good practice, particularly for the evaluation of advanced multi-agency projects involving data sharing.

The deficiency of effective evaluation tools is demonstrated by Finland, where 90% of agencies have outlined specific goals in their e-government plans, and 87% have strategies for achieving them; however, only 50% of agencies included strategies for both monitoring the achievement of goals, and evaluating the outcomes of the implementation they carried out.[50] Australia has identified management and governance of cross agency systems as a future priority, however, existing governance arrangements are solely single agency. Agency chief executives are legally responsible for using funds only to discharge the duties of their own agency. They may not therefore feel able to participate in whole of government strategies, and certainly

49 *UK Criminal Justice System Makes Portfolio Management Key to IT Success* (Gartner Industry Research, October 2005).

50 *OECD E-Government Studies,* op. cit., p. 73.

have a good excuse not to. There is an analogous problem in UK administrative law (see chapter three).

In Norway, agencies' e-government efforts are reported, but not assessed against any implementation targets (which sometimes do, and sometimes do not exist). The privatisation of Statskonsult, the government's analytical service, has increased the deficiency of evaluation of Norwegian e-government.

There are frequent and strong monitoring and evaluation procedures in Mexico. Unfortunately, these evaluations are dedicated to goal monitoring, and the goals reflect best guesses, made previously at a high political level. The strong evaluation procedures thus fail to monitor performance, or to provide incentives for performance based on customer priorities. Though strong, such monitoring procedure can result in perverse behaviour, such as the delivery of unnecessary on line information about services relevant to people with limited Internet access. There is also insufficient use of cost-benefit analysis to evaluate outcomes for the sake of allocating scarce funds to those schemes delivering highest value to customers.

Where data sharing is a specific project aim, there is at least a clear outcome against which to test the results. However, defining successful data sharing will present its own specific difficulties – it is unlikely that mere measures of the flow of documents will suffice to evaluate such a project. This is certainly an area where the UK will have to lead rather than learn from international best practice. The effort will certainly be easier if we ensure that new priorities are well aligned with existing demands on time, resources and effort.

This evidence suggests that further details of the implications of *Transformational Government* for particular departments must be worked out in concert with the comprehensive spending review and public service agreements. Taking advantage of the UK's sophisticated inspection and audit regimes, as encapsulated by Ofsted, the Healthcare Commission and the Audit Commission's comprehensive performance assessment to ensure PSAs set to support cross departmental action for *Transformational Government* will also be key.

Proposals

Incorporate the aims of *Transformational Government* into the formulation of PSAs, by identifying specific priorities for interdepartmental co-operation and the data strategies to realise these.

These priorities would be revealed by the assessment process described above, with the award of additional funding generating specific PSAs to deliver outcomes (such as fewer contacts with case managers) which can only be achieved by information co-operation.

The growing numbers of joint PSAs reflecting the needs of service and customer groups need to incentivise appropriate data sharing as a process crucial to improved delivery.

We should measure the outcomes not the process of data sharing. Joint working could be assessed with reference to repeat enquiries, or to transaction times, or to the accuracy of delivery, but *not* by reference to the number of items of data shared.

Chapter Five: The new localism? Reconciling central leadership and local enthusiasm

Introduction

There are two purposes to this chapter. For those who are unfamiliar with the progress of data sharing in the UK we discuss how CJIT and Connecting for Health have developed. This is important as it reveals a learning process sometimes alleged not to exist in government IT management. Combined with international evidence, this suggests a way forward for the difficulties experienced by CfH. The proposed combination of central standards and local implementation will be familiar to practitioners, but not perhaps to all those in policy making circles. Policymakers, however, will recognise a familiar debate about the central recognition of local priorities and autonomy, even in this specialist field. Those familiar with the CJIT and CfH experience may wish to move straight to the section dealing with how central standards can be imposed without "bullying" devolved agencies. This section discusses how we might graft the adoption of such standards into existing performance assessment frameworks, which are well-established means of cooperation between central government and specific agencies or localities.

The 'central-local problem' exhibits a scaling effect: it is relevant when considering the role of central government – the Cabinet Office, CIO Council and Treasury – in relation to the central departments (Whitehall); it is relevant when considering

the relations between the central departments and their agencies; and it is probably relevant at an institutional level in the relationships between managers and their staff. We concentrate on the department – agency scale of the problem, as this relationship has driven most IT and data sharing structures and has generated the most evidence. Towards the end of the chapter we offer some observations about the potential role of central government in driving data sharing. This role requires more than defining common standards, advice on *when* as well as *how* to share may be crucial to the realisation of *Transformational Government*.

Overview

Early IT investment programmes in the UK were characterised by a high degree of local ownership. These programmes struggled to make progress towards an integrated view of service users and as a result delivered patchy services. Yet the highly centralised programmes which replaced them, such as *Connecting for Health,* have recently experienced large-scale delivery setbacks and problems with stakeholder engagement. Where can the government go from here? In this chapter we look at trends in the purposes and management of e-government initiatives in order to make some suggestions regarding the balance of local-national initiatives.

ICT programmes often require huge organisation change, the introduction of new infrastructure and processes. This change clearly requires central coordination and direction, but experience shows that acceptance of such change by staff charged with implementing and operating new systems is crucial for success over the long term. The OECD identifies a central strategy as an important enabler of change, but state that to be successful, this strategy must be clearly communicated to lower level agencies. Owning this strategy and driving progress towards it are important functions of central government. Countries with traditionally independent and innovative agencies (Scandinavia and Australia) are increasingly discovering a need for improved central direction; whilst countries (such as Mexico) where strong central leadership has driven initial catch-up in basic ICT investments, are increasingly recognising the need to foster local level leadership and buy-in, so that more advanced ICT systems can enable organisational change.

Britain has recently developed an overarching national strategy – *Transformational Government.* However, the implications for specific departments remain uncertain. The Cabinet Office and CIO Council are strengthening the position of the government to provide central leadership. Central leadership at this level could either develop a guidance and framework-setting role, or develop strong oversight of agency level projects, following the recent British pattern for strong central direction.

However this pattern, culminating in *Connecting for Health,* has recently led to difficulties with the agency highly criticised for alienating doctors, running over budget and developing unnecessary products, based on an unhelpful architecture. Clearly stakeholder engagement has been a problem, though not all the criticism is justified. Future information sharing projects will require much better engagement with staff if they are to enjoy the transformation of business processes that will be necessary to support IT investments. It is therefore crucial that we understand how we arrived at highly centralised management structures such as CJIT and CfH, before we attempt to move beyond them. Understanding why we have such agencies reveals their strengths – strengths which future projects will need to maintain, even as we look for new models that can combine the advantages of central programmes with improved engagement with front line staff.

There is a good deal of international evidence, as well as UK experience, concerning the strengths and weaknesses of both central and local management. Together this evidence suggests the UK would do well to explore the ground between early highly localised strategies and recent highly centralised ones. The evidence then helps us offer some pointers as to how we might get there.

In this chapter we will attempt to understand:

- the role of national IT strategies in driving change
- the role of targets and the communication of strategies to local level
- the importance of collaboration and leadership at the highest level of policy development

- the strengths and weakness of both central and local management models.

Patterns of central and local control – lessons from abroad

Finland has relied on highly centralised planning combined with very local implementation since introducing e-government reforms in the 1990s. There is a widely recognised plan for an information society that fits coherently with wider public sector reform, suggesting effective collaboration at the top of government.

However, informing government employees of what this central vision means, and getting them to act on it, has been less successful. Some agencies have not translated the vision into local action plans. The OECD found a lack of targets *within* agencies and ministries by which to judge progress on the e-government agenda. The OECD felt that such targets would help drive implementation, and improve accountability. Despite this, the OECD praised the absence of quantifiable *national* targets. Generic national targets have led to difficulty in some countries, where resources have been poured into the effort to meet arbitrary deadlines and provide services for which there is little demand. This may suggest a boundary of the target exists: effective ICT targets may need to be developed near the operational front line, to ensure they are usefully aligned with customer required outcomes.[51]

In Norway, where delivery has been driven from the bottom up, there has been success, particularly in back office reform, but there are limits similar to those experienced in Finland. Norway does have a guiding strategy document. However, most administrators draw on an earlier document and vision based on a plan no longer in effect.[52] This suggests two possible problems: a) Norwegian leadership has not successfully communicated reasons for abandoning the old plan, or provided guidance for the shift to the new one; b) the old plan was perfectly acceptable and the centre have created a new vision which does not help administrators, so they stick to the old one. Problem a) would lead to people implementing unnecessary services e.g. 24/7 services for which there is no demand, problem b) would lead to confusion and would be detrimental to the delivery of the original, effective strategy. Either way, there is

51 This message was confirmed by *To the Point: A Blueprint for Good Targets* (SMF, 2004).

52 *OECD: Norway Assessment,* op.cit., p.3.

clearly a disconnect between highly autonomous local agencies and central strategists.

Further, ministries in Norway do not provide much guidance to the agencies on how to translate the national vision into action plans. Successful cross-ministry working between the Ministry of Labour and Government Affairs, and the Ministry of Trade and Industry, while harmonious from the point of view of the centre, has not produced a sense of clear guidance or leadership from the point of view of local delivery. These ministries swapped portfolios regularly and did not communicate agency responsibilities clearly. Again, the OECD identified an absence of ministry and agency level targets or goals as a major feature in this missing communication.

The Norwegian response to the need for improved central coordination has been to designate the Ministry of Modernisation as sole ministry with responsibility for e-government. This places e-government responsibility squarely with those responsible for public services modernisation. The OECD suggest that the success of this initiative will be contingent on deciding which areas of policy need central guidance, in order to support continued decentralised implementation, and which do not.

Swedish e-government reform is driven by a "24/7" strategy for guiding developments towards customer focused, e-enabled service delivery. The Ministry of Finance is ultimately responsible for e-government. However, the typical Scandinavian model of highly autonomous local agencies has resulted in a fairly decentralised e-government programme, and uneven development in different localities and areas of the administration. Efforts to improve central coordination have led to the creation of the *24/7 Agency Delegation:* a multi disciplinary, multi agency, multi sector working group, dedicated to producing technical solutions, funding suggestions and knowledge transfer patterns that can enable agencies to deliver on the 24/7 strategy. The aim is to harness and coordinate local enthusiasm, not to crowd it out.

Conversely, Mexico has strong central leadership in e-government. Ministers and agency heads discuss annual budgets with the president himself, and set e-government implementation targets as part of the process. E-government has been cen-

tral to good government and improved accountability drives in Mexico. E-government is thus well integrated into public service reform at the highest level. This has driven the first stages of improvement, but if investment is to yield returns through changes in working practices, there is a pressing need to develop more institutional and lower level enthusiasm for, and understanding of, e-government reforms.

Lessons learnt

1. a national strategy is important to inspire and coordinate local efforts
2. targets close to the level of implementation can be extremely useful in translating these strategies into local priorities
3. bottom-up enthusiasm for change is critical for back-office renewal
4. high level coordination must be effectively communicated to the local agency level or efforts will be wasted
5. central control should complement local delivery
6. strong *and* distant management and targets can be counter productive.

How does the UK's experience compare to this international evidence?

From local control to central control – the UK experience

The centralisation of network design and IT budgets (discussed above) went hand-in-hand in the UK with the realisation that large-scale national investments demand dedicated national leadership. Both CJIT and *Connecting for Health* provide this leadership on specific large projects, while the other main departments now have dedicated IT teams, whose leaders enjoy the same management seniority they would in the private sector (from where most are recruited). There are some signs that this approach is yielding results across government. The DWP inherited the IT confusion of the Child Support Agency – hardly auspicious for a department then charged with modernising the payroll technology of the entire benefits system. However, this challenge was successfully met under the supervision of a dedicated central IT team, with director general level leadership.[53] Arriving on time and on budget, the transition from

53 *Department for Work and Pensions SR2004 Efficiency Target. Technical Note, December edition* (DWP, 5 December 2005), p. 8.

paper book to direct debit payments should save the department £1 billion a year by 2008, as well as helping efforts to combat fraud.[54]

Given the necessity of centralising budget management and network design, creating powerful central units to carry out these tasks was understandable. Such central management structures were conspicuously absent from the original *Information for Health* strategy, and were progressively strengthened, especially after the Wanless Report highlighted local managers spending funds on other areas and not engaging with the IT programme. The programme delivery eventually became the highly centralised *Connecting for Health* in April 2005. Likewise, the original criminal justice IT reforms centred around a rather vaguely defined committee, termed IBIS (Integrating Business and Information Systems), which was replaced in 2002 with the rigorously structured CJIT. In both these programmes more rigorous, centralised management structures have proved capable of delivering results. This suggests that powerful bodies, imposing national uniformity, have done much to overcome the inertia which dogged the highly localised early efforts to digitise information sharing networks. This is clear from the progress achieved under *Information for Health* and CfH.

Information for Health envisaged connecting all computerised GP practices to NHSnet and completing the national email project by 2000, and seeing the NHSnet used for bookings, referrals, lab requests and results in all parts of the country by 2002. None of these targets were delivered, though others, such as the roll out of NHS Direct, and the enlistment of trial sites for patient records, were. Comparing this experience to CfH targets we can see that: connections to the new N3 network are running ahead of schedule, Choose and Book software was delivered on time, QMAS to support new GP contracts was delivered from 2004, on time, and is used by all GPs. Overall, CfH has reached more of its targets than previous management structures, but there remains a glaring problem: Deployment of the Care Records Service (the key product of the new IT programme) in trial form has slipped from December 2004 to late 2006 at the earliest. One of the key reasons for this slippage is a symptom of a wider problem, which we discuss below. In short, the UK is in a reverse position to most other advanced e-gov-

54 Estimate relayed by Pensions Minister Stephen Timms in 'Department for Work and Pensions is revising supplier contracts to slash costs through standardisation', *IT Weekly,* 12 January 2006. 'Instrument of payment fraud' (fake order books) was estimated to cost the department £46 million in 2004 (*Annual Report,* DWP, 2005, p. 64).

ernment countries: The UK has recently enjoyed some benefits from strong central management, rather than from active leadership at a local level. But we must consider the clear problems associated with this high degree of centralisation.

Problems with the UK model: divorce from front line staff

In March 2006, the GP community challenged the IT leadership of Connecting for Health, and, on grounds of concern for patient confidentiality, refused to accept the compulsory timetable for transfer of patient records from paper to electronic format. Now trials will not begin until the end of 2006 at best, with the full form being tried possibly in 2007. The transition had been intended to take place with an opt-out clause for those patients who felt threatened by the changes; the GPs forced a reversal and uptake will now be opt in – this could delay uptake significantly, it may improve public confidence, but it may reduce the usefulness of the service due to the potentially slow rate of uptake as people remain with the status quo.

Implementation that occurs later than is technically possible highlights the key problem with highly centralised management structures. Highly centralised, command and control-style programmes can easily become divorced from their local product users. Central management will usually design to an original brief – developed without extensive consultation with front line staff – and then dedicate their efforts to rolling out the technology created. It is not typically the responsibility of IT professionals to negotiate with end users, or to communicate progress and potential benefits to them. Even less attention has been paid to mechanisms by which end users can evaluate products and influence their further design. In CJIT and CfH, roll-out timing decisions have been wholly removed from front line practitioners and dictated by technical possibility. While such inflexible timing is understandable given the emphasis traditionally placed on delivering on time, it can be counterproductive when it exacerbates the distance end users feel from the products they will be expected to use. This can lead to a lack of cooperation from practitioners, introducing new delays to implementation. For example, after doctors' debates about opt in vs. opt out systems slowed the progress of patient records, one of their chief negotiators reported strong feeling 'that [the delay] is no bad thing.'[55]

55 Nicholas Timmins, Public Policy Editor,'Doctors' Debate Delays Patient Record', *Financial Times,* 27 April 2006.

At its worst, divorce between designers and users can lead to the development of poor or irrelevant products. If front-line staff are not consulted regarding the data they need on a day-to-day basis in order to fulfil their roles, it is more than likely that the operating systems and data sharing protocols they are given will not be fit for purpose and will require ad-hoc adjustments further down the line, a very expensive process.

Even where products are still relevant and high quality – as may yet be the case in National Programme for IT in the NHS (NPfIT) – we have seen that such divorce between users and designers makes implementation difficult, introducing unhelpful extra risk and cost. Rejection by professionals undermines the possibility of developing new business cultures and practices which, even more than developing new systems, is what data sharing requires. There is an additional complication when data sharing does involve new technology. When rejection risk materialises, the cost to contractors can be large. For example, in March 06 Accenture prepared to lose £450 million through the delay in NPfIT, difficulty in seeing a profit at any point has led them to bow out of the contract from 2007.[56] They are certainly not the only supplier to find major government contracts difficult. The government already faces difficulty securing interest from many major technology contractors. Management structures that exacerbate the risks of designer/user divorce and its associated hold up problems will only make the government less attractive as a source of business for systems integration companies. This is particularly true of smaller firms who could add some much needed competition and diversity to the supply chain.

While Connecting for Health has experienced considerable difficulty through its isolation from practitioners, CJIT, which is perhaps even more rigorously centralised, has not experienced such problems. This is perhaps because CJIT comes closest to replacing and extending an existing paper based data sharing system, the business needs it services are well established and there was extensive initial consultation on the ideal information needs of the various agencies of the Criminal Justice System. CJIT has suffered some delays, but its overall level of success may not be easily replicable if such rigorously centralised structures are employed to deliver more controversial or complex

56 'Accenture's NHS Losses Grow as NPfIT Delays Mount', *E-Health Insider,* 29 March 2006. Andrew Charlesworth, *'Accenture Bows Out of NHS Contract',* http://www.vnunet.com/ 29 September 2006.

changes to business practices.

The Care Records System (part of Connecting for Health), by contrast, envisages considerably more information sharing of highly confidential data than had previously existed. Despite the deficiencies of the existing paper system, this perhaps seemed to GPs – whose reputation for confidentiality is central to their success and who have a quite different relationship to their users than servants of the Criminal Justice System – to be a wholly new and dangerous business practice about which they had not been sufficiently consulted. Similarly, efforts to update intelligence and information sharing between police forces, in the wake of the Bichard Inquiry, have met some difficulty in dealing with the highly localised nature of power and operational priority in the police.

Summary:

1. Early (pre-2002) UK evidence, and subsequent international experience demonstrates the limitations of excessive localism for the development of high level, integrated, customer focused services.
2. UK experience since 2002, and Mexican evidence, demonstrates the dangers of over centralisation.
3. Therefore, we need to combine the advantages of central coordination and standards with some local control of product design and delivery timetables.

The patterns and developments in the relationship between central guidance and local implementation discussed above are summarised in Figure 1 below.

Figure 1. International approaches to guidance and implementation.

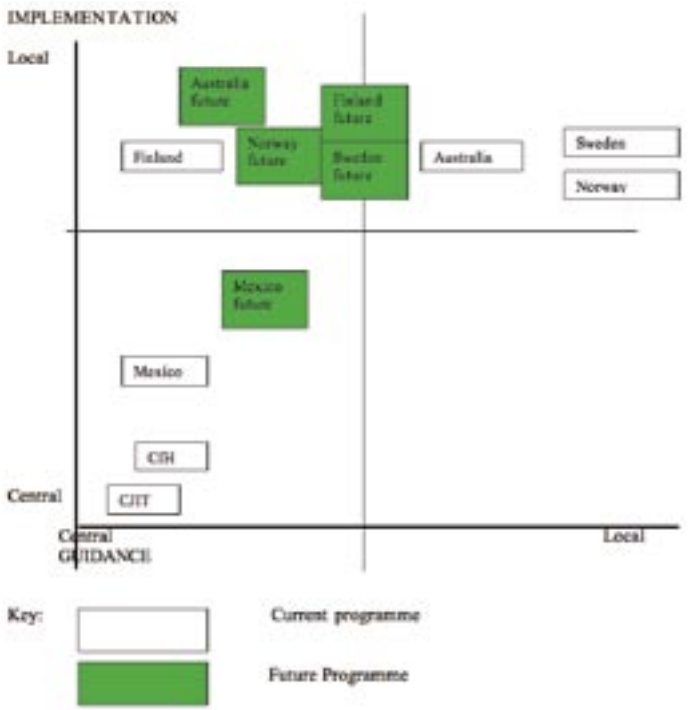
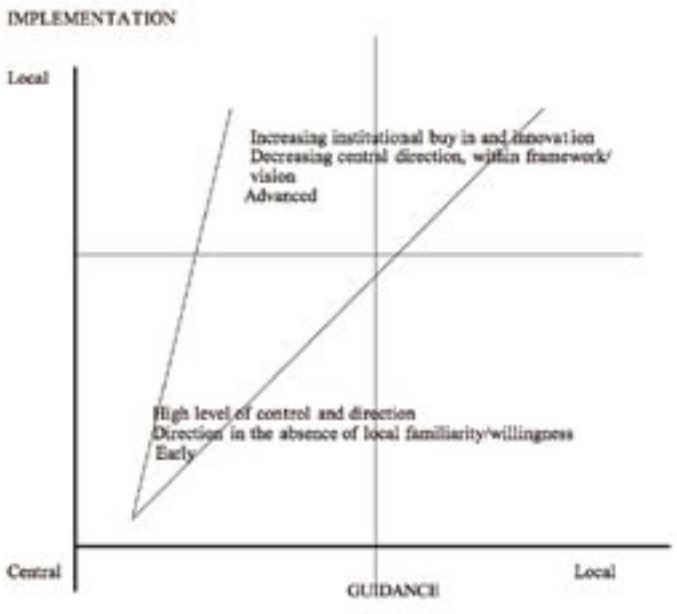


Figure 2 offers some explanation of these patterns, suggesting most countries are converging on a model with central visions, central standards for information and interoperability, and some local control over design and implementation.

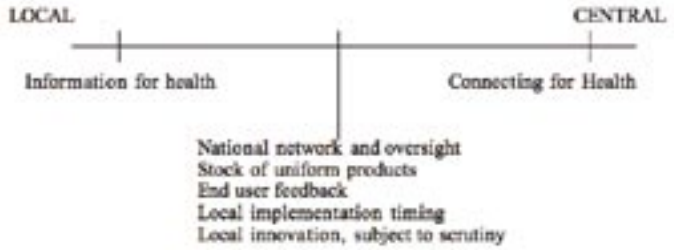
Figure 2. The direction of travel?



Defining a new middle ground

We have seen the benefits powerfully managed central programmes have delivered, compared to their decentralised forebears; yet they introduce significant new risks to the design and procurement process. It may therefore be useful to think less about two mutually exclusive options, and instead about management possibilities on a spectrum: from highly localised to rigorously centralised structures.

Figure 3. Spectrum of centralisation



In the middle ground is an as yet under-explored area: where rigorous national standards and interoperability are combined with a local autonomy that allows practitioners to implement standard products in the timescale most relevant to their local business circumstances. This process could enable early adopters to influence future redesigns, leading to the continual improvement of products and increased practitioner satisfaction, which may ultimately lead to better service delivery to users. Such intermediary centralisation is not the clear-cut solution to the specific problems of localism that complete centralisation has offered in the past. Rather, intermediate solutions would reintroduce some of the uncertainty characteristic of local flexibility, in order to avoid the larger risks which develop in highly centralised, complex and distant management structures.

We can think of this as replacing large single risks, such as the practitioner revolt experienced by Connecting for Health, with smaller, more manageable uncertainties around the specific uptake rate and locations of a particular product on a particular date. Furthermore, as we mention above, the UK has sophisticated and well developed inspection and performance management regimes in all of its public services. It would not be overly expensive or complex if the local implementation of national products and processes were to be monitored by, for example, the Healthcare Commission or the Audit Commission as part of their current regular inspection duties.

Different data sharing systems, and IT solutions generally, will fit best into different parts of the local-central management spectrum. Where to place new projects will be a hugely important decision and one that can only be made on the basis of the particular case, considering the products to be developed, and the existing administrative structures, rather than just previous successful or struggling programmes. Aligning the priorities of strategists with those charged with delivery will be key to this process.

Responsibility for police information technology strategy will shortly be transferred to the National Policing Improvement Agency (NPIA). NPIA is answerable to, and far more driven by the Association of Chief Police Officers (ACPO), than previous police technology organisations, which were answerable to the Home Office. Given the local account-

ability of chief police officers, and their significant independence, the ability of central strategists to drive local implementation is limited. This has probably hampered previous efforts towards interoperability and better information sharing, even in the wake of the Bichard Inquiry. With its ACPO driven remit, the NPIA is therefore in an improved position to deliver local cooperation towards national priorities than any previous body. Coverage so far has certainly been positive 'We stand more chance of success with the NPIA because there will be a single owner'.[57] NPIA is guided by the priorities of the Association of Chief Police Officers and may well explore this middle ground: where local purchasing decisions and feedback are combined with central product design and broad, flexible framework for product uptake. Given that the Police are far more locally autonomous than even doctors, this responsiveness to local priority, combined with the inclusion of local IT performance in the performance assessment of Chief Constables, is probably the only way national, coordinated IT leadership can be married to the extremely local incentives and priorities of individual police forces.

Figure 4. Position of programmes on centralisation spectrum.

Scaling up – the role of central government in our framework

In central government (Cabinet Office, Treasury, CIO Council) IT leadership has already moved towards the development of strategic visions and standard frameworks for interoperability to facilitate data sharing. These are represented by *Transformational Government* and the *e-Government Interoperability Framework* (eGIF), respectively. This is certainly encouraging; we have already seen that a central vision is crucial to a country's progress towards a better use of information across government. eGIF lays the foundations for making data sharing technically easier and is also a positive step. However, vision

57 Superintendents' Association chairman, Rick Naylor, quoted in Sarah Arnott, *'Doubts Linger Over Police IT,* Computing Magazine, 28 September 2006.

and standards alone do not communicate the high-level strategy to the departments and agencies that must implement it. Even with *Transformation Government,* even with eGIF, and even with the incentives and framework discussed earlier in this report, data sharing will still be difficult because departments and agencies may require guidance on *when* as well as *how* to share data. Within the framework suggested in this report, that means guidance about identifying the benefits of data sharing and then developing a business case from these.

We do not suggest that data sharing be driven by technical opportunity – the whole first section of this paper is about avoiding that possibility. Within our framework, however, we feel there is a strong role for a body, probably the CIO Council, in developing a centre of expertise in building organisational and commercial models to facilitate data sharing. We believe a robust and open process for assessing the strength of a business case for data sharing is crucial to both public confidence and rational investment. Building these business cases will be a challenge. Developing a central store of expertise, with particular skills in identifying and valuing the benefits of data sharing, will be an invaluable aid to real progress on the ground. Central government should not only develop a vision of integration, but also drive progress towards this vision by providing the specialist skills necessary to negotiate a framework capable of enhancing both public acceptability and professional freedom.

Proposals

At department-agency level
Central leadership and setting of minimum standards needs to be combined with local buy-in and the co-production of targets and standards, as well as the design of projects. This will minimise the risk of practitioners feeling divorced from the process and will lead to more relevant and useful IT products. This will involve:

- front-line input in the specification of new products
- aligning central and local accountability structures
- some local control over timescales for implementation.

At central government level
CIO Council, Cabinet Office and Treasury continue to develop the strategic vision and technical architecture for integrated government and data sharing.

CIO Council also develops a centre of expertise in identifying benefit cases for data sharing and building business and organisational models for the realisation of these benefits. This facility is there to cooperate with, and support, the departments involved in any given model.

Chapter Six: Managing relationships – challenges of data transfer and relationship management

Introduction

In this final chapter we consider some of the more technical aspects of data sharing. This will be of most interest to people concerned by the practical possibility of doing data sharing well.

Improved delivery and efficiency cannot be achieved simply by allowing practitioners to access records freely from other departments. There are three important processes that must take place if records are to be effectively and responsibly utilised by practitioners: data matching, agreeing common terms and coordinating responsibility for data quality. These technical considerations, explained below, support the argument made in Chapter one: that the associated costs and logistical challenges of data sharing will be most usefully pursued between limited clusters of services, where a strong business case can be developed.

The data-matching problem

Records referring to a particular individual need to be made unique, and consistent through changes over time. Within single record keeping systems this is easily achieved by "tagging" a record referring to a particular individual with a unique key: for example, "J Smith; 0123". As this John Smith changes his address, family status, benefit entitlements etc, these changes can be entered on his unique record, rather than that of the

many other John Smiths.

When two different institutions first start trying to share data, they generally have two different methods of tagging their records. For example, Department A's records may include "J Smith; 0123" while Department B's records may include "J Smith; ab4x". The unique key employed by Department A is different to that of Department B. Based on this information alone, it is not possible to establish if the two records refer to the same individual, or to two different John Smiths. Matching must therefore be performed on a set of fields held by both systems, eg name, date of birth, address etc. Matching on such fields is an uncertain business due to data quality issues and the need to find a set of fields that provides a unique match. For instance, one system may hold "J Smith" and another may hold "John M Smith". What additional fields are needed to uniquely match these two records? The matching system will typically generate both false positives (matches that actually represent two separate individuals) and false negatives (failures to match two records that should be matched). We can tune the sensitivity of the matching depending upon what use will be made of the matched data and our tolerance to false positive and negative matches.

When this problem applies to a population of millions, the workload involved in matching the correct John Smiths in each system to a particular John Smith in the real world is extremely large. This matching requires dedicated software and will frequently require manual intervention to resolve uncertainties when they arise.

As we have seen, the best-developed data sharing initiatives so far have largely upgraded existing paper-based data sharing networks. These paper-based networks have generally had consistent tagging routines in place. For example, patients' records are all tagged with a unique NHS number, and have been for some time. As such, the data-matching problem was not really a barrier to data sharing within the health service. The problem which necessitated an IT based solution was that it was very difficult to achieve the timely transfer of records between palliative institutions scattered across the whole country, several of which can be involved in the treatment of any one patient. Likewise, the CJIT team faced a huge backlog of infrastructure and effective business routine, but the case files of individual criminals were consistently tagged, removing the need to match data when the system become digitised.

However, data matching is a fundamental element of data sharing between departments, and even between some systems within departments. Not all data sets are as coherent as NHS records. Within individual departments, there may be several generations of records, with incompatible tagging systems. Across several departments, the problem multiplies. As noted, this can produce large error caseloads where serial numbers, names, addresses, etc., have been miss-keyed or wrongly assigned. Dealing with the errors requires judgement: when can a record reasonably be assigned to a particular identity and when is it no use and must be discarded? Judgement is expensive, especially if it requires training people, rather than software, in specific tasks. Errors are also embarrassing and spending significant sums of money correcting them, or discarding data, is not always a popular course of action for a public administrator (sometimes such an exercise is referred to as 'data cleansing'). Discovering large amounts of erroneous data immediately generates a further task – replacing the bad records with up to date, accurate ones. Data gathering too, is expensive and can alienate well-meaning service users, without any guarantees of catching those who, for example, are deliberately avoiding tax authorities.

Once a set of records from two or more different departments has been assigned to a particular identity, they need to be given a commonly agreed tag. Practitioners in both or all departments can then pull up all relevant information about that identity. This common tag may be based on one of the existing systems, or be created from scratch. This creates a further problem – which tagging system to use, or whom to charge with developing a new one? There is a great deal of interdepartmental politics involved in settling any discussion of this kind, whatever sector of the economy or institutional environment it takes place in. Using an existing number brings the benefits of familiarity for service users and some practitioners; it may reduce the number of records needing to be tagged with a new identifier. But existing numbers may be extremely insecure, especially if they are in very common use, and as such are not

suitable tags for highly sensitive information – it would be too easy for unsuitable people to quote the correct tag for an identity and access sensitive records, and information becomes more vulnerable the more its unique identifier number is used by different services.

If two services engaging in data sharing are of a very different nature, they may not feel the partner's identity tagging system is suitable for their service users (even if these are the same people, only in a different role). One service may worry about being tarnished by the negative associations people attribute to another service's identity tagging system. For example, the care services may not wish to be associated with enforcement and public protection services, when undertaking the sensitive data gathering that accurate care depends on.

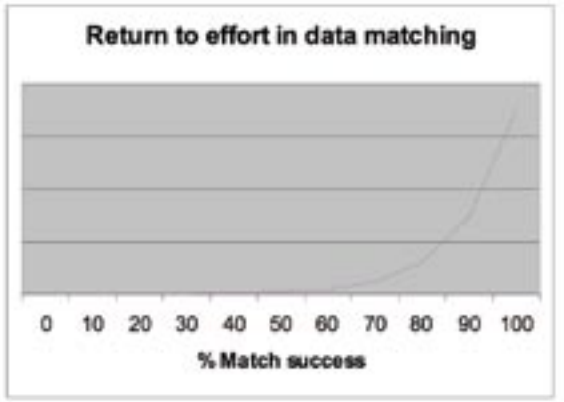
Where one department is closely associated with a particular tagging system, it may be assumed they have some sort of ownership of, or responsibility for, all data so tagged; this may or may not be appropriate in the particular circumstances of any given data sharing arrangement. The proliferation of different data tagging systems is a natural consequence of silo driven data organisation. However, the above considerations ensure that reconciling these different systems will be a difficult and politically sensitive task.

Resistance to undertaking the expensive, unpopular exercise of data cleansing, and the complexity and expense of subsequent processing is one of the reasons why government information has remained resolutely bound in departmental or agency driven silos for so long. Significant benefits would have to follow from the deployment of networked information systems to justify a large data matching workload. Sufficient benefits are probably only now becoming available, with better connectivity and database technology.

For example, the transactional departments seem to have a clear business case for data matching. They require much of the same information, for similar purposes. It would make sense for HMRC and DWP to be engaged in extensive data sharing, as it would be easier for citizens if DWP could update HMRC about changes in address or status of which it became aware – say if someone's earnings decreased to entitle them to tax credits, or if someone achieved an income which no longer required support.

It would be useful for these departments to check that details held about individuals were consistent with legitimate use of the tax and benefits system. Coordinating the records held on each individual and business by DWP and HMRC could therefore lead to significant improvements in transactional efficiency and service quality. There may also be cost efficiencies in the long run. As a result, there is a strong case for pursuing data sharing as the costs of the necessary data matching exercise are likely to be recouped.

In short, any data matching exercise will be expensive and difficult and it will generate false positives and negatives, with potentially serious consequences. The more effort (money) is invested in the exercise, the lower the probability of error. There is no one correct balance – some processes such as CRB checks require more effort than others – say perhaps, the identification of fraud. The difference confidence standards required for different processes are one reason for suggesting that different service clusters undertake different data matching exercises.



An alternative to piecemeal data matching is a universal data matching exercise, where all government data is joined up. One advantage of this would be that whenever departments decided data sharing would be advantageous, much of the preliminary effort in matching records would already have been done. Furthermore, all departments would be confident that

any data-sharing partners had well-ordered, up to date records. This would considerably simplify the problem of designing contracts, or other formal protocols, to govern relationships between data sharing departments.

However, there are serious problems with this method that would far out weigh the potential benefits. First, the cost would be enormous. Second, this cost may not be recouped for many years, as it is not clear that *all* government processes would benefit sufficiently from an ability to share data with *all* other government processes, to offset the cost of preparing for such a universal initiative. Third, it is not clear which identification number would be best placed to tag all individuals' records in all departments. There are several candidates: the NHS number – most of the population have already been assigned one of these; the National Insurance Number (NINO) – this is the most widely used identifier, the closest we currently come to such a universal tag; the Home Office's National Identity Register Number (NIRN) – if the ID cards scheme goes ahead as planned, this will be universal, difficult to acquire in support of fraudulent multiple identities and more secure than NINO. Choosing a tag could be solved with suitably high-level leadership, and some observers do see the emergence of a single common tagging system as the eventual outcome of current drives towards the efficient use of information.

There is a further danger that the creation of such a universal identifier may generate additional security concerns. While such dangers are present with any data sharing system with matched data, they must be balanced against the efficiency and service improvements realised through the sharing. In the case of universally matched government data, the potential costs of crime and error are very much higher than in more limited data sharing scenarios. It is not clear that the benefits realised would offset the costs of the necessary security. Security itself could impose data sharing barriers and verification procedures, which would slow down the transfer of data, compromising the very initiative they are supposed to protect. The more secure we try to make a system, the more cumbersome its operation may become. It is therefore highly unlikely that universally matched data would be an efficient solution to the data-sharing problem.

Proposals

Data matching should only be attempted where agencies demonstrate a clear business case for the benefits that they can provide to customers through greater data sharing, as we explain in chapter One.

Use of common data identifiers should also be limited to service clusters, identified by the frequency of daily interactions. For example, social services could increasingly use the NHS number, as improving communication between different care services is an acknowledged priority, while HMRC and DWP could coordinate data about individuals with NINO and the Home Office use the NIRN across its many diverse enforcement agencies.

The key aim would be to enable data sharing where it would strongly support the delivery of key services, while maintaining the existing assumption of non-matched data between agencies with little reason to communicate about any given individual.

Agreeing common terms

To transfer data between two systems, there needs to be an agreed format of data and interpretation of each data field – a "data model". The eGovernment Unit's eGIF standard goes some way to establishing this for commonly used data types, however further work is likely to be needed where wider data sharing is being introduced.

Next there is the problem that the systems use different ways to reference the same things. For example, different clinical terms may be used as shorthand for any given condition; the drugs prescribed to a patient may be referenced differently – chemically, by name, by maker, by local nickname. Individual institutions tend to develop their own shorthand and coding systems for the complicated information they record in the course of their daily business practices. Internally this is fine, but problems can arise when practitioners with different indexical knowledge access information coded in a non-agreed manner.

In such cases, records that are going to be shared beyond institutional boundaries must be transformed according to an

agreed set of descriptions. Again this adds cost and complexity to the data-sharing problem. Managing the translations between these terms requires the maintenance of a "reference data system", holding this mapping between the terms. Reference data systems need to be updated by all participating parties as new terms are established (for instance when a new drug is launched). In industries, such as the capital markets, where new terms are created many times a day, the management of reference data has become a significant problem and expense.

Government has already undertaken perhaps the largest task of this type likely to be encountered. The NHS NPfIT requires all medical records held by GPs, mostly on paper, to be re-keyed electronically, with conditions described according to a standardised national rubric. The necessity of this exercise was identified in the first *Information for Health* strategy paper, and a committee set up to lead the development of the national rubric.[58] Where this problem arises it can always be addressed, but will always impose costs.

The cost of any work to ensure the agreement of terms must be taken into account when deciding whether to invest in data sharing. Similarly the cost of maintaining the data model and reference data system must be taken into account. As in the data-matching problem, this technical consideration suggests there will be a natural limit to the efficient extent of data sharing across government.

Responsibility for ensuring the agreement of terms must be assigned to a particular body within the data sharing system – which brings us on to the broader task of data quality coordination.

Coordinating quality assurance

Who is responsible for ensuring that each element in a record held on a shared system is accurate and up to date? What constitutes an acceptable level of detail in an accurate entry? How regularly must records be checked to ensure they are up to date? There are no generic answers to these questions. Different business processes face different challenges and requirements. For example, transactional departments, such as HMRC, have to make a pro-active effort to keep track of contact details; care services, such as GPs surgeries, generally do not. Where effort must be expended to ensure data is up to date and accurate, the division of responsibility will have to be carefully worked out. In any given system, responsibility for some process-specific information may clearly rest with a particular professional; for example, treatment details may be the responsibility of the administering doctor. It is less clear who, in a shared data system, is responsible for keeping contact details up to date – is it the last institution to have contact? Is it the first? Is responsibility designated to a particular institution within the system, or should some new institution for 'basic data' be created to underpin the multi-service data-sharing exercise?

Again, the answer will vary depending on the partners involved and the nature of the data-sharing exercise. What is clear, however, is that upholding data quality is an expensive process requiring strong governance. In open access data sharing systems, this may create a "free rider problem".

58 *Information for Health. An information strategy for a modern NHS 1998-2005* (Department of Health, 1998).

Data sharing and the free rider problem

People want to enjoy the improved decision making and administrative efficiency that arises from improved access to high quality information. People do not want to incur cost and effort in order to maintain data quality, say through regularly updating contact details or using improved interview techniques. People can maximise their payoff from the system by providing information of a lower grade than that of other people. Individual sub-standard inputs do little to reduce the overall quality of information available, but save the individual involved significant time and effort. The individual thus accesses a high quality product – produced largely through other people's effort – while minimising the costs of his or her participation. Conversely, there is no incentive for anyone to take on the extra costs of supplying unusually high grade information to the system: the benefits would be small, as the higher grade information would be a small proportion of the total, and only a fraction of the benefits would accrue to the person making the extra effort.

Large institutions already find it difficult to ensure data quality. Where there are many people responsible for data input, an individual institution will develop governance structures to monitor the work of its data input officers. However, any given

institution in a data sharing system faces an incentive to free ride (or at least "cheap ride") on the effort of other institutions. Institutional and departmental budgets are often tight in the public sector; there is always a strong temptation to get more for less. Over time such behaviour may degrade the quality of information in the system, leading to bad decisions and costs in correcting errors, potentially making the information useless. These costs, however, would not necessarily accrue to the worst offenders, so their existence alone would not provide an incentive for institutions to improve their effort.

As individuals and institutions tend to discount future costs too easily, we cannot assume that institutions, under time and budget pressure to perform *now,* will act in each other's long-term best interests. Data sharing systems require governance mechanisms capable of ensuring that all information provided is of agreed quality, and capable of enforcing penalties if it is not. Existing oversight regimes, limited to single institutions or departments within a data sharing system, will probably not be sufficient to guarantee this in a cross-departmental context.

To overcome this problem we must look at some key questions:

- Should departments with the most routine use of a certain type of data automatically assume ownership for this data, and guarantee its quality?
- How can receiving departments confirm data quality and complain if it is insufficient?
- How can responsible departments recover any increased costs of taking that responsibility?
- Do we need a central information department to take ownership of all public sector data? Or merely to oversee contracts between data sharing departments? Or at all?

We feel the costs of establishing a new department of information are probably too large to consider at the current stage. However, organising rights and responsibilities to and for data will be crucial to the success of any new information sharing strategy. We have already suggested that departments with most interaction with a given customer group are probably best placed to take responsibility for data sharing systems relevant

to those service users. Below we make some tentative proposals for how rights, responsibilities and compensation could then be organised.

Possible solutions to upholding data quality

To ensure data quality, access to information should require the fulfilment of certain conditions. For example, access to shared information may be granted in return for the provision of high quality data to the system. It would be the task of the data owning body to vet information entering the system, at least until a source becomes established, when checks might become infrequent. In other words the monitoring would be risk based. The central department whose agencies have most to do with the information of the customer group whose data is being shared would be the logical candidate for ownership of the data and probably the system holding the data. Local offices could be linked directly to the system or they could be linked through their controlling agencies, which would then be responsible for ensuring data quality before passing information on to the system for further verification.

With rationalised data collection, some agencies/offices would be responsible for supplying specific information to the system. Other institutions could use this information, and concentrate on supplying different data. It would not generally be possible for different institutions within the public sector to exchange information of equal value – they would therefore need further compensatory mechanisms. For example, information could be traded through the system. Those public bodies freed of finding information themselves could pass some of the accompanying savings to the organisations who *were* providing data, to compensate them for the extra effort they were making to provide high quality information. Concentrating the search and collation of specific information in one set of institutions, rather than duplicating it across the public sector, would greatly reduce the overall cost of information acquisition to the public sector.

The operation of such an internal market warrants furthers investigation because no department would have a large enough incentive to shoulder the whole burden of information collection without some form of compensation. This compensation

could also be organised through departmental budgets, settled by the Treasury. However, trading the information with regular departmental compensations would offer a more dynamic method than annual, or triennial Treasury settlements. As more information was consumed across the public sector, more effort could be invested in its collection by the responsible department. Likewise, a price gives the receiving institutions some power over the supplier – if the quality of the data supplied is not adequate, they could withhold the compensation payment, and the supplier of the information would notice in their budget. This would give the responsible department a strong incentive to supply high quality information to the system. The lead department, probably that whose agencies (and their local offices) supply the most information to the system, could be responsible for net settlements across the system, should this prove more efficient than multiple bi-lateral settlements.

Clearly there would be expenses associated with the operation of a price mechanism; any such market would be far from perfect, requiring additional regulatory machinery. Particularly important expenses would be the settlement technology and the ability of participating departments to monitor the quality of the data. Careful cost benefit analysis needs to take place before government pursues this, or an alternative solution, such as adjustments to Treasury settlements. There could also be a problem with the public perception of departments "buying" data about citizens from each other. If such a market solution were to be pursued, government might have to undertake a considerable amount of public education about why this mechanism was being adopted.

These considerations point to a very important fact – even if a price system could be used to arrange compensation between cooperating departments, such a system could not alone guarantee data quality. Neither could Treasury settlements, as these are fairly infrequent events. Therefore there will be an important role for regulation in data governance.

Either a price system, or a Treasury settlement system, would introduce some mechanism for control over the terms of supply and consumption of data (by introducing an implicit form of contract, and mechanism for redress). As well as this high level structure, additional data governance measures would

be required. This creates something of a problem as most public sector inspection frameworks deal with service provision, rather than the central departments (for example, Ofsted does not inspect DfES). Bodies capable of holding central departments to account have traditionally been limited to the Treasury, the National Audit Office and the Audit Commission, but the Cabinet Office is also now developing such a role, through the capability reviews.

There would be two steps to creating strong data governance procedures:

1) It would probably be necessary to establish formal Service Level Agreements (SLAs) against which the data owners maintain the data and to which they are held account, and Terms of Use (ToU) which describe how the data can be used (or any limits or boundaries of its use), against which consumers of data would be monitored and held account.
2) We would then need a mechanism for monitoring these agreements and holding parties to account. This would form the next level of a data governance framework and could be arranged in several ways:

One possibility would be to create a governance forum formed of both the owners and key consumers of the data within a data-sharing cluster. This group would be charged with monitoring data quality, reviewing its use, and assessing new applications to use the data and their impact on the data collection and governance regimes. Such a group would be a new cross-departmental institution. Creating such groups would be a large undertaking; they would need a remit, resources, and some method of inspection and enforcement. Inspection and enforcement could be pursued in two ways:

- Governance forums could be created with executive powers of inspection, and powers to administer penalties such as financial penalties, public censure against offices or lead individuals, or other forms of sanction.
- Governance forums could be created with powers of inspection/data collection but without the power to provide sanctions. However, they would then need the power to appeal to some

existing body capable of enforcement, such as the Treasury, National Audit Office or Audit Commission.

This second option would perhaps allow the governance committee to concentrate on considering applications for the new use of data, and their effect on the data-sharing business case, governance and data collection regimes. It would be possible to subject the work of the governance forums to further democratic oversight, submitting their work to the Public Administration Select Committee, for example, if this was felt desirable. While the question of *when* to share data should rightly be assessed in the public eye, data governance within an agreed sharing mechanism is more routine and may not be the best use of select committee time. The Information Commissioner's Office could conceivably have a role in assuring data quality, given that the DPA enshrines citizens' rights to accurate, up to date information. Once again, however, we would have to consider the existing commitments of this institution before charging them with new responsibilities.

An alternative arrangement, following this logic, would be to create a forum of data owners and users, without executive powers, specifically to consider strategic issues in the development of data sharing within the cluster. If cooperation, rather than enforcement was the main aim of such groups they could perhaps be established as offshoots from the CIO Council, a body which already includes the Chief Information Officers of the central departments.

We would then have to establish the monitoring and maintenance of SLAs and ToU through existing inspection/performance management frameworks.

The key performance management framework for central departments is the system of PSAs, which are negotiated with the Treasury. It might be possible to use these in relation to data governance, particularly if the Treasury takes responsibility for compensations between data gathering and data consuming departments, as the two could be negotiated simultaneously. PSAs are usually numerical, so could take a form something like "Department A to provide data at x% accuracy rate to Departments C and D". However, PSAs are generally used to reflect an aspiration, a target, rather than to ensure the

59 http://www.audit-commission.gov.uk/performance/index.asp?page=index.asp&area=hpbvpi

maintenance of an existing level of service. Also, PSAs may be negotiated infrequently, possibly only triennially with the comprehensive spending review process. Both these considerations may make PSAs unsuitable for the day-to-day detail of data governance, though they could certainly have a role in providing headline visibility for the quality of key data used widely by other services.

To monitor performance against SLAs and ToU requires a body with the ability to collect and review the quality of information provided departments. One way of approaching the data governance problem would be to look for an existing institution that already has similar capabilities, so as to minimise expenditure on the acquisition of new competencies. The Audit Commission already reviews the quality of information gathered and published by central departments and local government bodies. The Commission has a particularly strong role in assessing the quality of information provided to the Treasury and Department of Communities and Local Gevernment as part of performance assessment routines.[59] Given that the Commission investigates information quality in the context of performance management; has powers to collect data from central departments and; has power to publicly report on this data, the Commission may be able to absorb responsibility for monitoring compliance with SLAs and ToU drawn up by data sharing departments. Departments in data sharing clusters could then agree to share data and provide suitable compensation (either through pricing or budget negotiations), subject to the satisfaction of the Audit Commission that the terms of the SLAs and ToU developed during the negotiations had been met.

Even if we wish to use the powers and expertise of the Audit Commission in the data governance process, it may be possible to do so without burdening the Commission with the actual inspection of the day-to-day quality of information being shared. When the Audit Commission reports on information provided by, for example local councils, it does not actually gather this information itself. Rather, the Commission provides guidelines on what data must be submitted to it by councils and then undertakes further work to check its quality and ensure reported performance indicators are consistent with this. We

could use a similar process to monitor compliance with SLAs and ToU. The CIOs of data sharing departments could be charged with reporting their assessment of their own, and possibly their partners, performance in terms of the SLAs and ToU to the Audit Commission. The Commission would then verify these reports and publish their findings. This system would keep most of the costs of enforcing compliance within the data-sharing cluster, while making use of existing expertise and enforcement mechanisms in the wider public sector.

Proposals

The government should explore the possibility of a market for arranging compensation between departments sharing data; or else the government must devise some alternative form of contract to compensate those departments whose responsibilities for ensuring data quality would grow following data sharing projects. The adjustment of Treasury settlements to take account of information flows between departments would be such a mechanism.

For essential areas of data, likely to be shared widely, the government should consider the use of PSAs on data quality for the lead departments, to provide greater visibility of the quality of data being shared.

Where data sharing occurs, the departments involved should establish appropriate SLAs and ToU as part of the data sharing case. Their actions should then be measured against these, with sanctions for non-compliance.

The government must develop an appropriate mechanism for undertaking this monitoring and enforcement. Several options for the location of these powers are considered in the text. Further work is needed to decide between them, but minimising the cost of compliance mechanisms would be an appropriate means for doing so.

Conclusion

We are frequently told we live in a digital age, an age of information. We have lived through the "third industrial revolution", a revolution in the storage, processing and use of data. More importantly, we live in the age of the consumer where the quality of a service is as important as the availability of the service.

Yet government's use of information, especially the personal information on which service delivery depends, remains bound by a code designed for ration book technology, one-size-fits-all services, and limited public expectations. If the government is to meet modern expectations of service quality, within a budget determined by an increasingly tight fiscal environment, it must change the way it handles personal information.

Why now?

This will be a difficult and controversial task. But it is a task worth pursuing because the ever-increasing pace of globalisation and technological change, which drive our economy, make government services more, not less, necessary. For example, making the benefits system work to maximise people's chances of re-employment is crucial to maintaining opportunity in open labour markets. To do this, in a modern skills based economy, would require an integrated approach to both benefits and training. If information about employment history and educational history are the preserve of separate groups of professionals and cannot be shared, such a constructive evolution in the nature of government services cannot happen easily.

This is just one example of how services could evolve to better meet modern challenges and better suit their diversity of users. It is not possible to think of all eventualities ahead of time. We therefore need a flexible information policy, a policy

that can allow government services to develop as the challenges faced by British citizens also change. Yet this information policy must still ensure that sensitive information is only available to those who need to know it.

To share or not to share?

A individual instance-by-individual instance system for authorising data sharing will never be flexible enough to allow the evolution of government services around the user; but complete freedom to share information will not be efficient and may compromise people's rights to privacy and the security of their data.

We believe the power to share data should be limited to those practitioners who are using the data to deliver clearly specified benefits to their service users. We believe this can be achieved by adapting existing government/civil service processes to serve democracy as well as delivery, making the business case a tool for democratic as well as technocratic evaluation.

Throughout the report we emphasise the opportunity data sharing represents to lay the foundations for an effective information society. Privacy alone is insufficient to guide our attitude to personal data in the twenty-first century. The costs of privacy (foregone services and higher priced services) will undoubtedly rise throughout the next decades. If we are to take advantage of technology and enable government services to develop as our needs change, we need a new basis for our information relationships with government.

Towards an information society: public service reform and information

Putting the user at the heart of the service has been the guiding principle of reform for a decade; it is a good principle and one that should be at the applied to information policy. Citizen centred information flows will not alone ensure effective data sharing. Extending individual information rights will be crucial to developing popular, secure data sharing. A new information policy is an excellent opportunity to lay the foundations for an information society with high levels of trust, openness, responsibility and oversight – and hence low levels of fraud, error and abuse.

At the moment we are a long way from such a society,

though Freedom of Information rights are an important first step. Information sharing should be pursued for the benefit of citizens, but different people will view the costs and benefits of information sharing differently. As far as possible, we need to allow people to make their own judgements by choosing whether or not to allow particular parts of the state to share their data. Personalised services will depend on personalised information relationships. Acknowledging this will be a first step towards greater engagement between citizens and the state in the information arena.

Taking the engagement further, we propose that individuals should increasingly own records detailing which agencies have accessed their data. This would enable people increasingly to police their own data. Crucially, it will also allow people to develop trust with data-sharing public servants who use their information responsibly and constructively. Trust and oversight, working together, could enable far more effective transactions than privacy alone ever would.

Further work

This report is a first step and probably outlines more questions than it solves. Particularly pressing priorities are

- further work on how to develop oversight and trust in data sharing systems, and how far technology can reasonably contribute to this
- a better understanding of how to identify and value the benefits of data sharing, in order to invest in the most high-value cases
- a process for identifying cross-cutting user groups.

We must remember that data sharing is not e-government (though there is overlap) and that no one project encapsulates the benefits of data sharing. We have tried to outline a framework which will clarify the possibility of data sharing for front-line public servants, and maximise our chances of investing in the most high-value projects. There are many forms of information that are not sensitive or personal and are not considered in this report, but they could be the best place to develop new technologies which may eventually help us handle personal information more effectively.

List of abbreviations

ACPO	Association of Chief Police Officers
APPSI	Advisory Panel on Public Sector Information
CfH	Connecting for Health
CIO	Chief Information Officer
CJIT	Criminal Justice Information Technology Unit
CNIL	Commission Nationale de l'Informatique et des Libertes
DCA	Department of Constitutional Affairs
DCLG	Department for Communities and Local Government
DfES	Department for Education and Skills
DPA	Data Protection Act
DVLA	Driving and Vehicle Licensing Agency
DWP	Department for Work and Pensions
eGIF	e-Government Interoperability Framework
FOI	Freedom of Information Act
GOL	Government on Line
GP	General Practitioner
GPS	Global Positioning System
HMRC	Her Majesty's Revenue and Customs
HRA	Human Rights Act
IBIS	Integrating Business and Information Systems
ICO	Information Commissioners Office
IT	Information Technology
MISC 31	Ministerial Committee on Data Sharing
N3	National Network
NHS	National Health Services
NINO	National Insurance Number
NIRN	National Identity Register Number
NPfIT	National Programme for IT in the NHS
NPIA	National Policing Improvement Agency
OECD	Organisation for Economic Co-operation and Development
OfSTED	Office for Standards in Education
OPM	Office for Public Management
PIU	Performance and Innovation Unit
PKI	Public Key Infrastructure
PSA	Public Service Agreement
QMAS	Quality Management and Analysis System
SLA	Service Level Agreements
SMF	Social Market Foundation
ToU	Terms of Use

References

6, P., Raab, C., and Bellamy, C (2005). "Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I." *Public Administration* 83 (1), 111-133.

Accenture's NHS losses grow as NPfIT delays mount. E-Health Insider, March 29 2006

Audit Commission. *Performance Indicators.* <http://www.audit-commission.gov.uk/performance/index.asp?page=index.asp&area=hpbvpi

BBC News website. *Counting the cost of UK fraud.* November 24 2005
<http://news.bbc.co.uk/1/hi/business/4463132.stm>

BBC News website. *Foreign criminals 'not deported.'* April 25 2006.
< http://news.bbc.co.uk/1/hi/uk_politics/4942886.stm >

'Building Local e-Government through Public-Private Partnerships: Conference Report.' *Information Technology in Developing Countries* 12(2)
http://www.iimahd.ernet.in/egov/ifip/nov2005/article7.htm

Cave, J (2004). *The economics of cyber trust between cyber partners.* London: Foresight, Cyber Trust and Crime Prevention Project.

Collins, B., and Mansell, R (2004). *Cyber trust and crime prevention project. Executive Summary.* London: Foresight.

Comptroller and Auditor General (2005). *Filing of income tax self-assessment returns.* Her Majesty's Revenue and Customs, National Audit Office

Council on Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens (2005). *E- Government in the member states of the European Union.* IDABC

Department for Constitutional Affairs (2003). *Public Sector Data Sharing: Guidance on the Law.* London: DCA

Department for Constitutional Affairs (2006). *Information Sharing Vision Statement.* London: DCA

Department for Work and Pensions (2005). *Annual Report.* DWP

Department for Work and Pensions (2004). *Data Sharing and Data Matching of Personal Information.* London: DWP

Department of Health (1998). *Information for Health. An information strategy for a modern NHS 1998-2005.* DoH

Dunleavy, D., and Bastow, S (2005). *Is measuring public sector productivity so hard? An application to local e-government change.* London: LSE Public Policy Group.

e-Government Observatory (IDABC), (2005) *e-Government in the Member States of the European Union.* Brussels. European Communities.

Gartner Industry Research (2005). *UK Criminal Justice System Makes Portfolio Management Key to IT Success.*

Home Office (2004). *The Bichard Inquiry Report.* London: The Stationery Office

Home Office (2006). *New Powers Against Organised and Financial Crime*.
<http://www.homeoffice.gov.uk/documents/cons-2006-new-powers-org-crime/cons-new-powers-paper?view=Binary#>

Information Commisioner's Office (2006). *What Price Privacy. The unlawful trade in confidential personal information*. London: ICO.

Information Commisioner's Office (2006). *Identity Cards.* http://www.ico.gov.uk/about_us/news_and_views/current_topics/identity_cards.aspx

'IT in public administration of Estonia'
<http://www.theregister.co.uk/2006/03/30/public_service_transformation_underway/>

Kablenet (2006). 'First phase of public service transformation underway.' *The Register.*
<http://www.theregister.co.uk/2006/03/30/public_service_transformation_underway/>

Office of the Deputy Prime Minister (2005). *Inclusion Through Innovation. Tackling Social Exclusion Through New Technologies.* London: ODPM

Office of Public Management (2005). *Research into the use of personal datasets held by public sector bodies.* London: OPM

Organisation for Economic Co-operation and Development (2003). *E government in Finland: an assessment.* OECD: Public Affairs Division

Organisation for Economic Co-operation and Development (2004). *OECD E-Government Studies: Finland.* OECD Publications

Organisation for Economic Co-operation and Development (2004). *OECD E-Government Studies: Mexico Assessment.* OECD Publications

Organisation for Economic Co-operation and Development (2004). *OECD E-Government Studies: Norway Assessment.* OECD Publications

Organisation for Economic Co-operation and Development (2005). *OECD E-Government Studies: Norway Assessment.* OECD Publications

Organisation for Economic Co-operation and Development (2003). *OECD E-Government Studies: The E Government Imperative.* OECD Publications.

Performance and Innovation Unit (2002). *Privacy and Data Sharing.* London: Cabinet Office, PIU.

Privacy International. <http://www.privacyinternational.org/>

Sarah Arnott. *Doubts Linger Over Police IT.* Computing Magazine, September 28
2006

Social Market Foundation (2004). *To the point: a blueprint for good targets.* London: SMF

Timmins, N. *Doctors' debate delays patient record.* Financial Times, April 27 2006

Wanless, D (2002). *Securing our Future Health. Taking a Long Term View.* Her Majesty's Treasury.