

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this consultation are primarily from the data protection perspective.

Our main involvement with information sharing projects is usually through our role as supervisory authority. This role can be as an advisor when approached over new information sharing initiatives or government policy, as educator in our activities to promote a high standard of data protection, as problem solver when dealing with complaints or as enforcer when we need to take regulatory action.

Providing a response on the use and sharing of information could potentially cover a very broad a range of issues. This response therefore focuses on the issues raised by sharing personal information.

[Empty box]

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

Question 2.

Comments: The ICO recognise that there may be benefits to sharing information, such as in the delivery of services and the convenience with which the citizen can access those services. Appropriate information sharing is also vital in combating fraud and some areas of crime prevention and detection.

Question 3.

Comments: Compiling and sharing large collections of personal data carries associated risks. There is an inherent security risk every time personal information is shared between organisations. There is a risk that poor data quality can result in a spread of inaccurate information about the individual or false matches of information provided by different organisations.

Gathering personal data on large numbers of people also runs the risk of intrusion into the private lives of individuals through the potential for profiling, matching, mining and interrogation of the data. In addition even where data is not “sensitive”, the gathering of personal data increases the breadth of the impact upon individuals where such data is compromised, sold to another company or shared with another department. Where data is collected to serve the needs of an organisation rather than the individual, it can also lead to a growing distrust and disconnection between the citizen and government or the customer and the company.

There might also be risks to individuals where personal identifying information is used in areas where it is not strictly necessary for the purpose. For example in medical research where there is a need to be able to identify that a series of events involve the same person, but there is not a need to hold information which clearly identifies the individual concerned (name, address etc.). Holding personal identifying information runs the risk of gratuitous disclosure and has greater potential for damage and distress to individuals where this information is lost.

Question 4.

Comments: Opportunities for improving the scope and methods of using and sharing personal information include greater use of Privacy Enhancing Technologies (PETs), use of authentication and hit/no hit systems, and more considered use of data minimisation as an alternative to widespread collection and sharing of personal information. In addition, the growing awareness of information assurance methods and the use of PIAs allow greater consideration of risk in relation to sharing personal information.

Risks include poor standards for using and sharing personal information and the poor quality of information being shared. These are not just risks to the

individual, but also to the organisation as they increase the risk that sharing the data will not meet business need. There is also the risk that sharing of personal information is being driven by expediency rather than a properly considered need.

In addition, information sharing is often viewed as an innate good in itself, rather than a useful tool for achieving legitimate aims. This has at times hampered debate about the risks inherent in an increase in collection and sharing of personal information. As a result, the potential exists for information sharing operations to go ahead without sufficient consideration of the risks involved and then without the accompanying safeguards to mitigate those risks. This leads to unnecessary costs being incurred on information sharing projects through building in safeguards later or making good on losses as a result of breaches.

Question 5.

Comments: The National DNA Database continuing to hold DNA samples on those who have volunteered data as part of a wider campaign or who have not been prosecuted or convicted has not been demonstrated as being necessary and proportionate to the prevention or detection of crime. Similarly, the development of the UK's "eBorders" programme, with widespread collection and sharing of information between a range of agencies has potential to be very intrusive into the lives of individuals but has not demonstrated the necessity or effectiveness of all the measures proposed. HMRC and other recent losses of personal information demonstrate the risks of an organisation sharing fields of information which have not been requested and are not strictly necessary.

Question 6.

Comments: The ICO is not able to identify private sector organisations who may be holding too much personal information. However, if it was clear that an organisation was holding too much information, holding it for too long or holding irrelevant information, then the ICO would take appropriate action.

The ICO has done a great deal of work with private sector organisations who hold large volumes of personal information, such as credit reference agencies, to ensure that the information they hold is relevant, adequate and retained only for as long as is necessary.

Question 7.

Comments: Attempts by the Government to document cases where information sharing is not happening, despite it being in the public interest, have not produced any clear cut evidence that there are legal barriers. There is some anecdotal evidence but where the ICO has been asked to comment, the barriers do not stem from application of DPA.

At one time it was thought that DPA was a barrier to sharing information for the purposes of records based medical research. However, the tort of breach of

confidence is a more prevalent concern for medical practitioners who wish to share information for medical research purposes.

Question 8.

Comments: Clearly the data protection principles demand that information sharing must be necessary, that the information provided must be adequate but not excessive and that the information is accurate and up to date, as well as being secure.

There is a proposal that Credit Reference Agencies would receive information about child support payments from the Department of Work and Pensions and would routinely share this with other credit providers when an individual has not paid child support. The ICO does not see the reasoning behind what began as sharing information about credit history now being used to collect other information on individuals which may have an impact on decisions made about them.

Another example is the Criminal Records Bureau providing all conviction information about an individual as part of a clearance check for working with children and vulnerable adults. While the ICO supports the sharing of information about offences which are of relevance, such as offences against children, more information than is strictly necessary is being shared.

Even where the case has been made to share information, the mechanisms and means of sharing are often where the risks involved in information sharing lie. Reports from HMRC surrounding the data breach have suggested that much more information was shared with NAO than had been requested. While we await the results of the separate investigation into this particular breach, it does highlight the wider problem of information being shared when this is not necessary.

Section 3: The legal framework

Question 9.

Comments: The data protection principles provide a common sense framework for sharing information. However, the complexity of the rest of the legislation has led to many myths about what is and is not possible when it comes to disclosing personal information. There is also some confusion over the distinction between data controller and data processor and the requirements around what constitutes “fairness” in relation to the first DP principle. There are opportunities to simplify the legislation, and the ICO has been involved with the Ministry of Justice on this issue. In addition, the ICO has taken a constructive and flexible approach to interpreting the law. This includes using powers under S51 of DPA to produce codes of practice which explain the requirements of the law and recommend good practice in clear and simple terms.

Question 10.

Comments: For historic reasons, the ICO has tended to focus on the issue of “fairness” in relation to the first principle in articulating the approach to compatibility with

stated purposes. However, the ICO believes the second principle is important to the working of DPA, but it is often misinterpreted or misunderstood. The word “incompatible” can be interpreted in such a way as either to prohibit any additional use of information or as enabling sensible, proportionate evolution of purposes that are not completely counter to the original purposes for which the data was collected. The ICO takes the latter interpretation, with the focus on ensuring transparency, accountability and proportionality. For example, where personal information has been collected to provide a service, it would be acceptable for that information to be shared to assess the processes involved in providing that service, such as through a customer satisfaction survey or for audit purposes.

In addition, the ICO is concerned that one of the means by which the purposes for processing can be specified is by providing the purposes as part of the notification given to the Commissioner under Part II of DPA. The ICO does not view this as sufficiently transparent and it causes confusion for data controllers.

Question 11.

Comments: At European level, there is a constraint on the scope of changes to DPA as our legislation has to be in accordance with the provisions of Directive 95/46/EC. The definitions in the DPA need to be addressed, in particular the definitions of personal data and processing, which have both been interpreted by the Courts in a manner which some have argued is not in line with the EU Directive 95/46/EC, and have perhaps led to more confusion as to where responsibility begins and ends. There is also confusion over where the line is drawn between a data controller and a data processor. At an institutional level, the DPA has sometimes been seen as a barrier or an obstacle, with training of staff and policy on the application of DPA within institutions not keeping pace with the development of new technologies and applications involving information sharing.

At a societal level, research shows that people want the benefits of data sharing. However, the ICO’s annual track survey in 2007 showed that there had been a significant decrease in the public’s faith that existing laws and organisational practices provide sufficient protection of your personal details, from 49% in 2006 to 39% in 2007. The public also showed high levels of concern about organisations holding personal information, in particular keeping personal information secure and selling personal details.

The impact of recent high profile losses of personal information on public attitudes has yet to be assessed. While not a barrier at present, if public were to lose confidence in the ability of government or private sector to use and share their information appropriately and securely, then this could become a barrier to sharing information in the future.

Question 12.

Comments: The ICO would like to see the provision for compensation in section 13 of the DPA to be extended to those who have suffered distress where they have not suffered damage. The ICO have submitted a paper to the MoJ in relation to further powers and penalties which should be made available under DPA. This

paper forms part of the ICO response to this consultation and can be accessed at.:

http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf

Question 13.

Comments: Often public bodies do not fully understand the nature or extent of their powers, which while leading to confusion over whether a particular act may be viewed as *ultra vires*, also impacts on the operation of the first data protection principle, and therefore also on sharing personal information. The common law of confidentiality may also be a constraint on sharing personal information and all public bodies, including the ICO, have to ensure that any personal information sharing is done in accordance with the Human Rights Act 1998. Thus convention rights, and in particular Article 8, must be considered where any information sharing initiatives are being developed, at least so far as the public sector is concerned.

As mentioned above, the ICO is keen to continue to work with the MoJ on simplifying and improving data protection law in the UK, but there is a constraint on the extent to which the law can be changed as the Data Protection Act 1998 has to properly transpose the requirements of Directive 95/46/EC.

Question 14.

Comments: The ICO should have the power to audit public and private organisations without it being necessary to obtain their consent. In addition, the statutory basis for information sharing needs to be examined. Often public sector organisations struggle over whether they have the powers to share personal information in any particular case while other bodies will often assume the powers exist and information sharing processes are put into practice without proper debate.

The ICO will continue to provide guidance to clarify the extent to which information sharing can occur, but does recommend that where information sharing has potential to significantly impact on the individual, such as may be the case in crime prevention or fraud detection, the information sharing should have a specific statutory basis. This should be done in such a way as to allow time for debate in Parliament to enable adequate safeguards to be put in place.

Question 15.

Comments: The ICO believes that DPA underpins good customer service and thus should not place a significant burden to those private organisations with a customer focussed policy. We have often described DPA compliance as “enlightened self-interest” as far as business is concerned. DPA will be a burden on those who have current poor practice who do not wish to change that practice, but this is not unreasonable.

Section 4: Consent and transparency

Question 16.

Comments: There is a great deal of difficulty when information collection and sharing is based on the consent of the individual. Consent can be withdrawn and obtaining individual consent to information sharing which is unlawful will not make it lawful. The conditions for processing detailed in Schedules 2 and 3 of DPA provide mechanisms other than consent for processing personal information, but as already stated, these can in themselves be confusing. However, the ICO view is that it is more important that any sharing of personal information is legitimate, necessary, proportionate and well thought out than that consent should be obtained in every case.

Consent and transparency are two separate concepts under DPA and linking the two can in fact devalue consent. For example, an organisation wishes to keep an individual informed and does this by asking for their consent. Where the individual refuses and the information is shared regardless, consent is a false notion. Some organisations have issued guidance stating that it is always preferable to obtain consent. However, where the information needs to be shared in order to deliver an essential service, this should be made clear to the individual as a term of business and should not be dressed as consent.

Where no other condition for sharing information is available, then it is important that consent is "true" consent. That is to say it is genuine, informed, freely given and can be withdrawn. There are different mechanisms by which consent can be obtained. Where the information sharing is not considered particularly intrusive, it can be sufficient to obtain consent via an opt-out, where consent is implied. The more intrusive forms of information sharing would require an opt-in, where consent is explicitly given. All forms of consent rely on the information about the proposed information sharing being clear and readily available to the individuals concerned.

The ICO considers that it is important that the concept of consent is reserved for situations where the individual has a genuine choice and it is not devalued by asking for or using consent where no real choice exists.

Question 17.

Comments: It is inadvisable for any organisation to base information sharing on consent. For the individual, suspicion and lack of trust are the main barriers for providing consent for sharing of information. For the organisations, the fact that the information sharing is reliant on the individual not withdrawing consent means that information sharing projects are at risk from a change in public attitudes or an organised campaign by interest groups or other third parties..

Question 18.

Comments: The ICO published a Framework Code of Practice for sharing personal information in October 2007. There is an entire section on fairness and transparency which includes guidance on drafting fair processing notices, the requirements to provide information on processing operations, keeping notices up to date and sharing information without people's knowledge and consent. In

addition, there are examples of good practice in other jurisdictions which could be adopted easily in the UK which could lead to increased transparency in sharing personal information. For example, in Belgium and Slovenia, individuals have online, real-time access to information about who is accessing and using their personal information and any changes to the data sets which occur. Other technological advances such as user centric identity management could also not just inform, but empower individuals by limiting information sharing to only the necessary information in each particular case.

Question 19.

Comments: Obviously the ICO sees great value in both tools and will be promoting the use of both tools over the coming year. Consideration should be given to a requirement for every major government initiative which involves sharing personal information to be subject to a full scale privacy impact assessment, with consultation with the ICO built into the process at an early stage.

Section 5: Technology

Question 20.

Comments: Obviously new technologies have made the sharing of information between organisations quicker, cheaper and easier, but the development of technologies which make information sharing safer and more secure do not appear to have kept pace with sharing technologies and are certainly not as prevalent. There is a danger that, with the ease with which information sharing can now occur and its obvious benefits, information sharing has come to be seen as a panacea of public and private service delivery, not merely as a useful tool in appropriate circumstances. There is also a danger that the procurement of high capability technologies is driving the development of information sharing, rather than a carefully considered and balanced evaluation of benefits and risks. In addition, the procurement of IT systems in different departments seems to have happened in silos at times, with no provision made for ensuring that IT systems across government are compatible so that legitimate and necessary information sharing can occur without undue difficulty or expense.

Question 21.

Comments: Mandating specific technological safeguards would be impractical as technologies develop so quickly that what is required this year may be obsolete or compromised by next year. Specific legislative provision would perhaps struggle to keep pace with the development of technology. Rather, and perhaps more practical, would be the introduction of an "Information Security" Code of Practice to be developed using existing powers by the ICO in partnership with other bodies such as CSIA. Taking a Code of Practice approach would allow the ICO to update the code as necessary, dependent upon the rate of technological development. Failure to adhere to the code would be taken into account when assessing whether an organisation has complied with the 7th principle.

Question 22.

Comments: If data can be anonymised and still be fit for purpose, then this is not just preferable but necessary under the DPA, as the processing of personal data must be necessary and not excessive. A good example of this is in the field of medical research, where the research often relies on the linking of a series of events which occur in relation to an individual, rather than relying on knowledge of the identity of the individual. There is also an argument for the greater use of systems which authenticate a right to a service rather than identifying the individual using the service.

The ICO view is that anonymisation and pseudonymisation should be considered where practical. The advantage of using anonymised or pseudonymised data is that the safeguards which need to be built into the processes are less than where the information identifies an individual as the risks are lower.

Greater use of identity management can be tailored to serve the needs of an organisation while at the same time informing and empowering the individual concerned. The ICO will be producing a paper on this issue which we will provide to the review.

A further example of where technology is being used to enhance the privacy of individuals is in the Austrian eGovernment initiative, where a system of fractional pins is allowing access to personal information across the public sector while limiting this information to that which is necessary for the delivery of a particular service.

The ICO feel that often these techniques and technologies are not considered due to fear of the unknown, the perception that costs of using this techniques would be prohibitive or that there is simply no incentive for using them.

Section 6: International comparisons

Question 23.

Comments: Other European countries have invested in prior checking of processing operations which involve specific risks to the individual. Privacy impact assessments are mandatory in the US and parts of Canada and other jurisdictions. In Canada and France, the Commissioner has the power to invoke a temporary or definitive ban on processing operations which do not comply with their domestic law. Certain jurisdictions can also issue fines, for example in France and Hong Kong. Across Europe and the Commonwealth, many regulators have the power to conduct an audit on companies without the consent of the company and have the requisite powers of entry and inspection to facilitate this. The Australian Taxation Office and assistance agencies must comply with the Data-matching Program (Assistance and Tax) Act 1990) and guidelines issued by the Privacy Commissioner under the Act to govern the conduct of data-matching using tax file numbers.

Question 24.

Comments: Online, real time access to information regarding who is accessing your personal data is available for all citizens in Belgium and Slovenia. This is relatively simple and inexpensive and would make a big change to the transparency of processing operations in the UK.

As already mentioned, the Austrian eGovernment initiative has introduced a series of fractional pins, which could be a good example to draw on for UK initiatives, such as "Tell us Once".

Question 25.

Comments:

Question 26.

Comments: There are differences in public attitudes towards sharing information across Europe. Former communist states have seen the public as very suspicious of information sharing.

Germany is considered to have a more restrictive data protection regime than some other European member states.

Section 7: Additional questions

Question 27.

Comments: This review should also address the resources provided to the ICO to cover the regulation of DPA in the UK. There may also be a need to look at providing further funding to information sharing initiatives where limitations on costs and resources may be standing in the way of providing adequate security and privacy safeguards.

Question 28.

Comments:

The Data Sharing Review

Richard Thomas and Dr Mark Walport

Additional submission from the Information Commissioner's Office

On 15 February 2008, the Information Commissioner's Office (ICO) submitted a response to the Data Sharing Review's (DSR) consultation on the use and sharing of personal information in the public and private sector. The ICO would be grateful if the DSR could also consider this additional submission as part of their review.

The Personal Information Promise

One of the key concerns we have is the perception that responsibility for the use and disclosure of personal information is not taken on board at a senior level. To that end the ICO is suggesting that heads of organisations or Government Ministers sign up to a 'personal information promise'. The aim is to demonstrate senior level commitment to data protection and by doing so drive up compliance and public confidence in the use of their personal information.

The 'promise' would list a number of key commitments that the senior figure would be making on behalf of the organisation. The 'promise' presents challenging commitments which show that the organisation they represent takes the handling of personal information extremely seriously and has mechanisms and resources in place to deliver on that commitment. We are aware that some organisations have adopted a charter for handling personal information in the past, but the focus of the pledge is to ensure that ownership and commitment at senior level.

We have drawn up a suggested promise as a starting point for further discussion. This includes 10 commitments.

1. We value the personal information trusted to us and we will ensure we respect that trust.
2. We will not only comply with the letter of the law when it comes to handling personal information, we will go further adopting good practice standards.

3. We will make sure that when we are planning to use or hold personal information in new ways, such as when introducing new systems, we will consider the privacy risks first and address these.
4. We will be open as possible with individuals about how their information is used and who it is given to.
5. We will keep personal information to the minimum necessary and delete it when we no longer need it.
6. We will have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands.
7. We will ensure that all our staff who handle personal information receive training and it is a disciplinary offence if they misuse or don't look after personal information properly.
8. We will regularly check that we are living up to our promise and we will report annually on how we are doing.
9. We will put appropriate financial and human resources into looking after personal information.
10. We will ensure that senior staff take responsibility for how we treat personal information and will make sure we can live up to our promises.

Clarity of roles

A second issue of concern to the ICO is the apparent lack of clarity of roles and responsibility for the management of personal information within Government. Clearly each department carries responsibility for specific activities that fall within its remit but it is not always clear where responsibility lies for issues which cut across departments. This extends not just to strategic matters such as Government wide policy on information sharing but also to more practical matters such as improving practice on the provision of fair processing notices. It is not always immediately clear to the ICO who we need to talk to if we are to achieve a Government wide commitment on a specific issue and who has the authority to deliver such a commitment.

If this is unclear to us, we wonder if it might also be unclear within Government as to where advice and guidance should be sought. We know, for example, that sometimes departments are uncertain whether it is ICO or the Ministry of Justice that they should be approaching. Given that the Cabinet Office and others also have an involvement there is scope for confusion. It may be that lines of responsibility are clear and it is only better explanation that is needed or the problem may go deeper.

17 April 2008

