

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: Personal data is collected about me.

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

Question 2.

Comments: There are no benefits which outway the disadvantages - eg I have a medical condition about which I do not want information to be shared.

Question 3.

Comments: The disadvantages have been vividly exem plified recently, with data on half the UK population going missing as well as other losses/ releases.

Any computerised system of information can be penetrated by determined hackers. Once identity information is stolen the individual will be faced with having to prove that they didn't do things, eg remove money from their bank accounts, against an insistence that the system is inviolable.

There will inevitably be 'function creep' - more and more agencies and hence increasing

numbers of people allowed access to data. The finding of illegal immigrants in the security services shows that there is no guarantee that all employees will be appropriate people.

ID cards would not have prevented the London bombings and if reports of the large number of plots being foiled are true, the lack of them is not seriously hampering efforts to prevent further attacks. Any organisation with the funds to mount a large scale atrocity will be able to get round ID card provisions. Identity theft from ID cards will be possible and provide the thief with even greater scope to make use of a stolen identity.

There is no guarantee that authorities will remain benevolent; hence a risk that in the future the powers that allow the collection of data for ID cards could be used for control and harassment. It puts too much information, and hence power, into the hands of the state and is creating a 'them and us' gulf between rulers and the ruled which is highly inappropriate in a democracy.

There are already indications that the data collected will be used not just for the benevolent purposes but also for punitive ones. Once they have given information and biometric identities away people will not be able to control what happens to them. Once a mistake is made the information cannot be withdrawn.

Question 4.

Comments: Computer-based methods because of the risks of unauthorised access and loss of data, neither of which can be fully protected against. Centralised data basis lay information open to a very wide range of people and the more agencies have access to it the greater the risk of penetration.

Question 5.

Comments: The problem is information sharing, whereby agencies have access to information not initially collected by them for purposes other than the ones for which people originally provided it. Public agencies should constantly evaluate what information they actually need - not want - to function and delete what they don't

Question 6.

Comments: Again the problem is not so much private businesses asking people to give them information as where they are enabled to access information not given directly to them; for example to medical records. That said, far too many companies on the internet ask for information such as email addresses when it is unnecessary from the individual's point.

People should not have to pay to gain access to information held about them, eg credit ratings. They should be notified that such information is being held and able to scrutinise their files freely and challenge inaccuracies.

Question 7.

Comments: I can't think of any.

Question 8.

Comments: Any sharing of information is unacceptable. If agencies need information they

should ask for it directly so that people know exactly what records are held about them by which body.

Section 3: The legal framework

Question 9.

Comments: The DPA is, in my experience, effective in ensuring that smaller scale organisations are careful with computerised records.

Question 10.

Comments: The second principle is too general and too easily allows for information sharing. If organisations really need information they should collect it directly and not through sharing. The costs involved would encourage them to ask if they really do need it.

The principle should be reworded along the following lines:

Personal data can be collected only for specific and lawful purposes. The reason for the collection of each item of information must be made clear to the person providing it. The data collected shall be used solely and exclusively by the body which collected it and only for the reason specified when it was collected.

Question 11.

Comments: Its remit is too general and not sufficiently focused on the privacy of the individual in relation to large institutions, particularly those of the state. It should exercise much greater control of what information is collected and should scrutinise any information gathering exercise to ensure that each item is genuinely necessary.

Question 12.

Comments: It should have greater powers of prevention and be able to require the complete destruction of data bases which do not comply absolutely with the law on data collection, especially in terms of the necessity for each specific piece of information. The costs of the destruction and reassembly of data bases would be a more effective deterrent than fines.

Question 13.

Comments: Yes but they are circumstance specific. It should be the responsibility of the DPA to take the initiative in scrutinising the nature of data collected and as far as possible preventing the collection of unnecessary or excessive quantities of data. There should be an absolute focus on 'need to know' and the public should be protected from being asked for information that is not absolutely necessary.

Question 14.

Comments: Information sharing should be ended. Organisations that require information should collect it directly and ensure that they ask only for information that is absolutely necessary for their purpose.

Question 15.

Comments: The emphasis should be on the protection of individuals, not cost-saving.

Costs are the most effective way of making organisations ask what information they really need and indeed whether they actually need it at all.

Section 4: Consent and transparency

Question 16.

Comments: The question should not arise. People should be asked for the necessary information by each individual organisation that requires it. That is the only way to ensure that they know how many organisations hold information about them, what it is and what it is for. That is the only way to ensure consent and transparency.

Question 17.

Comments: Information sharing should be prohibited.

Question 18.

Comments: Organisations should be required to collect information directly from individuals and make clear the reasons for asking for each piece of information. People should have the right of access to all information held by any organisation collecting it from them and the right to challenge it free of costs. Every person should be invited by each organisation every year to check, update and correct the information held about them.

Question 19.

Comments: Though well intention these do not address the main problem of information sharing, ie the spread of information not necessary to the receiving organisation and the fact that people are unaware how far their information is spread. Prohibiting information sharing is the only effective way of ensuring that people are able to know what organisations hold information about them, what information that is and the purpose to which it will be put.

Section 5: Technology

Question 20.

Comments: The constantly evolving technology involved in identity theft has had the effect of making it dangerous to the individual for too much information relating to individuals to be held in any one place. Organisations should hold only the information absolutely necessary to them, in order to limit the amount held in any one place and make it easier to detect where leaks come from.

Question 21.

Comments: Specific technological safeguards would be the subject of intense disagreement, as is at present the case with ID cards. They would also be rapidly overtaken by technological advances. Organisations should be liable to prosecution for negligence by the DPA if information goes missing or is stolen or misused. The head of each organisation should be personally accountable for ensuring that data is protected, along with a senior staff or board member with direct responsibility for data protection. The DPA should be well-funded to ensure that it can carry out its primary function of protecting the public,

individually and as a whole.

Question 22.

Comments: Such techniques are constantly evolving as is the ability to break through them. People should give necessary information direct to any body wanting to use it so that they know who has what and can monitor for themselves as well as being protected by such devices - that way individuals can be notified if there is a breach in security, because the organisation will have records of who provided it.

Section 6: International comparisons

Question 23.

Comments: The United Kingdom is the most watched in Europe, with more information held, in more forms, about more people than anywhere else on the continent. What we can learn is how to make do with holding a lot less information.

Question 24.

Comments: No - personal information should not be shared.

Question 25.

Comments: No - personal information should not be shared

Question 26.

Comments: One instance is that then American people would be so hostile to the idea of ID cards that neither President Bush nor any presidential candidate has dared suggest it.

Section 7: Additional questions

Question 27.

Comments: I am a member of the sector known as 'members of the public'. I am appalled that this exercise has been aimed at those with a vested interest in data collection and sharing. The 'general public' are second from bottom of the list of people it is aimed at, which is indicative. Many questions have been phrased in a way that could deter people from expressing their views and or guide people to respond in a particular way.

Question 28.

Comments: This review appears to be predicated on the notion that information sharing is a given, so how to dress it up to give people confidence in it. A primary concern seems to be cost-saving.

The costs involved in having to collect data for themselves direct from individuals and justify the need for each piece of information requested would make organisations think much more carefully about what they really need to know. It would prevent information given in good faith for a benevolent purpose then being used for punitive reasons. It would provide transparency because people would know what information was being held about them, by whom and why and be able to challenge its accuracy and misuse.

Data sharing is a major threat to individual privacy and liberty and undermines the balance of the relationship between the citizen and the state. The concern should be to redress this balance by reducing the amount of information held to a minimum and ensuring it is available on a strictly need-to-know basis and only for the purpose for which it was collected.

Your declaration of disclosure does not make clear precisely who could have access to this material and for what purpose. You specify the Ministry of Justice - what about other government departments, such as the security services?