

# 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](mailto: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: My interest in information sharing is twofold, partly because I work in IT and have the need to provide data security for client information and databases, and I am also interested in how data sharing affects everybody.

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

Question 2.

Comments: The key benefits of data sharing could be in providing accurate and speedy services efficiently.

Question 3.

Comments: There are many risks in data sharing because it increases the probability that sensitive data can get into the wrong hands. We have seen some high profile cases where such data has been misplaced. If such data does get into the hands of criminals it can easily help with fraudulent activities, such as Identify Theft.  
In addition, since some of the information will be incorrect (no system is perfect), then this incorrect information will also be shared. We have already

seen a person's car crushed for not having insurance when, in fact, they did have the insurance. The information shared with the Police was incorrect.

Question 4.

Comments: The risks start with the information that is captured and then how it is stored. If stored on a computer, it is often possible to gain access to the information without having physical access to the computer (unlike paper based records). The more information is shared then the greater the possibility that the data is misused.

Question 5.

Comments: It is hard to answer this question without knowing exactly how much information is actually held by the public authorities. I would suspect that they already hold more than they need, judging by the information that was alleged to be present on the child benefit disks lost by the HMRC.

In my view there should be the following rules in all organisations to reduce risks:

- Organisations only capture and store information that they need to carry out their core functions.
- Stored data should be distributed so that it is difficult to access to all of it at once (don't store it all in a single database).
- When giving information to another organisation or department, only the data that is needed should be sent and not whole databases.

Question 6.

Comments: Organisations often ask for too much information. I have often been asked for my date of birth or home telephone number when these organisations have no need for it..  
(I don't wish to give my DOB because this is used by my Bank for security purposes and I don't wish to give out my home phone number because this is likely to lead to "cold calling").

Question 7.

Comments: I can think of one example where data sharing may be more convenient: The Tax office has all my details of income etc, but I have to separately tell them this information again if I want to claim Tax Credits. It would save time if they could share this information. However maybe the convenience is not worth the security risks.

Question 8.

Comments: The obvious example was the lost HMRC disks. Detailed information was stored on these disks, even though only much less was actually needed by the NAO.

### **Section 3: The legal framework**

Question 9.

Comments: The DPA is a good idea but it does have some loopholes:

- Some encrypted personal data is currently exempt from the Act. This should be

remedied.

- More should be done to protect children's personal data. For example they should be more restrictions on schools taking biometric data from children, especially for trivial purposes such as library systems and dinner queues.

Question 10.

Comments: Some organisations do not hold well to the second principle of the DPA. For example private companies can sell your information on to other companies for "marketing purposes". Although you can opt out, many make this very difficult by using techniques like hiding the opt-out box in the "small print".  
The second principle of the DPA is an extremely good idea for reasons I have already stated in my answer to question 5.

Question 11.

Comments: Ignorance is often a barrier to such rules such as the DPA. Many companies, and especially in the public sector, employ low paid staff to carry out important work. Often training is an afterthought. Therefore mistakes are made and rules are broken. I don't think it is possible to eliminate mistakes completely, so any legislation must take account of this, but few laws actually do.

Technical barriers include poorly designed computer systems, which make it hard for employees to get the job done, and have ill conceived security models. This is the norm rather than the exception since few organisations will pay the price of doing it right. I have seen this many times in my capacity of IT consultant, where clients insist costs are cut.

Question 12.

Comments: My answer to question 9 should partially answer this question. In terms of sanctions they should be set at an appropriate level to work. For example there's no point having a fine of, say, £5000 if it would cost the organisation more than that to comply. It must be set at an order of magnitude higher.

Question 13.

Comments: I broadly agree with the EU Directive 95/46/EC and the OECD's recommendations on the protection of private data. It is important to evaluate the effectiveness of all such guidelines, recommendations and legislation to make sure it is working as expected and to correct any problems and not assume that everything is ok just because it was done for the "right reasons".

Question 14.

Comments: There should be greater protection for individuals as I have already stated in my other answers. Any legislative changes should only be done after proper consultation and in a proper democratic manner.

Question 15.

Comments:

#### **Section 4: Consent and transparency**

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments: I'm not convinced that it is desirable to make data sharing more transparent. Individuals should have the right and the opportunity to have more control of how, when and where their personal information is used. Organisations do need to do more to explain why they need so much information and how they can ensure it is secure. Individuals should have the right to inspect and correct any such information at no cost to themselves.

Question 19.

Comments: Policy can be developed with proper scrutiny and accountability if all stakeholders are given a chance to express opinions and that those opinions are valued and not ignored. Also this process must not be rushed so that all have a chance to assess the impact. The Information Commissioner's recently published Framework code of practice for sharing personal information looks valuable. However there is a danger of having too many documents that many will never read. Better still to boil it down to the basic principles, such as the seven principles from the OECD's recommendations for protection of personal data

#### **Section 5: Technology**

Question 20.

Comments: Technological advances have improved the speed of access and the amount of information that can be stored. This has streamlined many activities, but has created new problems. Sensitive databases can and have been hacked by criminals the other side of the world. It can be very difficult to trace these people and even more difficult to bring them to justice. Databases and large computer systems are still new to many and few people understand them properly. I feel that often, technical solutions are "thrown" at a problem by lay-people who are impressed by the technical buzzwords.

Question 21.

Comments: Unfortunately many organisations have not secured their data properly voluntarily so, perhaps, legislation may be necessary. When it comes to portable devices then the information must be encrypted to a very high standard. Better still to restrict or even outlaw the storage of information on portable devices. Encryption and decryption technology progresses very fast and care must be taken in any legislation to cater for the possibility that an encryption algorithm is only assumed secure until such time as it is proved not to be. You can't prove the positive.

Therefore any such legislation must be reviewed and updated at very frequent intervals. Also legislation should take account that data security by encryption can only be assured for very short periods of time, even assuming that no major advances are made in decryption techniques. This is due to computers increasing in power all the time.

Question 22.

Comments: 'Privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, may help safeguard personal privacy. However care must be taken to ensure that identities cannot be derived by cross referencing with other data sources. Therefore it should only be used if other methods (such as aggregation) are not possible. I am confident in pseudonymisation techniques but it appears many are not. As usual time and money constraints would often stop such options being used.

### **Section 6: International comparisons**

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

### **Section 7: Additional questions**

Question 27.

Comments:

Question 28.

Comments: One thing that cannot be stressed too much is that the information stored and shared is not always 100% accurate. However too many people take this information as "gospel" even in the presence of contradictory indicators.

People must be educated to consider the accuracy of all such data and systems using such data must have the resilience to cope with errors.

It is very important to get the balance between privacy and data sharing right. Things have swung too far to favour large organisations over the individual's rights. This needs to be addressed urgently. People must have more say about what happens to their own personal information.