

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: As an individual I have a bank account, credit cards, use the services of many companies, shop online, use the NHS, submit tax returns and pay taxes.

As a company director I am responsible for the safe keeping of the personal information that the company collects.

We collect phone numbers, next of kin contact details, credit card numbers and passport numbers of our staff, which are given voluntarily, in order to assist them in emergencies during field trips. We also have their bank details, used in making salary payments to them.

We collect email addresses, phone numbers and correspondence records from information given to us by our customers, for use in corresponding with them. We may also have records of their bank details in our company bank account

statements and on payment advice forms.

We collect standard logs from our Internet services, including web sites and email servers, which are used by the general public and by our customers. We do this in order to comply with data retention laws, to maintain operational efficiency and security, and to diagnose and repair failures.

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

Question 2.

Comments: Companies may sell information to each other or exchange it to make a profit and to reduce the risk of fraud. For example, company A may collect information on customer X, which it sells to company B, and uses the profit of this sale to subsidise the cost of providing services to X. Similarly, if company A detects that X is committing fraud, it can prevent the fraud and therefore reduce its costs to other customers.

The fraud argument applies to sharing information between government departments. This sharing may also help to detect other types of crime, such as terrorism, and to increase the chances that essential medical information will be available in an emergency if a patient is unconscious.

The benefits to individuals might be cost savings from companies, slightly lower taxes, slightly lower risk from terrorism, and a slightly lower risk of death in case of a medical emergency.

Question 3.

Comments: The main risk to individuals is the loss of control over information which they consider private. Such loss may happen by accident (loss of disks or laptops) or be the result of criminal activity (unauthorised access to computer systems, eavesdropping, interception, bribery, physical theft).

The main risk to society is that a large number of people become conditioned to loss of privacy and to providing whatever information they are asked for, and whatever the government is able to collect without their assistance (e.g. road camera records, phone records, Internet access records) and that it becomes increasingly impossible for those of us who value our privacy to keep it.

This has already happened to a large extent, and it is now all but impossible to use the NHS, pay taxes, own a house, have a job, buy online, drive or fly anywhere or own a television without giving personal information to companies and the government.

Data sharing increases the chances of government detection of crime. Since nobody is innocent, this increases the risk to all of us. Threat of exposure of illegal, immoral or disreputable activity is often enough to silence those who are

inconvenient to the government through their desire to protest against government activity. This is the route to a police and surveillance state, as seen in 1984.

Such systems are also liable to false positives, which prejudice falsely against those who are least able to defend themselves, such as those without money, good English skills, familiarity with our system and society, supportive friends.

Some things which are now considered a crime, such as demonstrating outside the Houses of Parliament, are actually fundamental necessities of a democracy and one who undertakes the planning or execution of such activities should not need to consider themselves in the wrong, or at risk of an anti-terror raid.

Many illegal immigrants are actually wronged by our system and have a moral right to stay, despite the government's efforts to detect and evict them which will only increase in severity.

Question 4.

Comments: Centralised database pose a massive risk by providing attractive targets and magnifying the risk of loss or theft. The larger the database, the more risky it is.

Databases of highly sensitive information, such as medical records, travel records and bank account records, are more likely to be harmful if released, and consequently more attractive targets and more in danger of release.

Any data sharing that helps the government to detect crime is likely to bring greater government oppression, especially of those who are least able to defend themselves, and especially where the accusations are false.

Question 5.

Comments: I believe that governments do not need to hold records of our Internet access. Real criminals and terrorists are perfectly capable of hiding their activity from the government, so those who suffer are those who commit more minor crimes or conduct immoral or disreputable activity, from adultery to music downloading.

I also believe that the government does not need to hold road traffic records from speed cameras indefinitely as they currently do, that it will not prevent terrorism at all and is only likely to be used for low-level domestic crimes of little importance.

I believe that the demand for biometric identity cards and passports is fundamentally at odds with a free society, and presents a massive risk of information theft and fraudulent abuse of such systems, as well as being an unbelievable waste of money and sold on the basis of the pure lie that it will help to reduce terrorism.

I think that everything the government does in the name of reducing terrorism is a waste of money and that if they want to reduce annual deaths, they should have a war on drivers and road deaths instead.

<http://injuryprevention.bmj.com/cgi/content/abstract/11/6/332>

Users of the NHS should be allowed to see their entire medical record history and to irreversibly delete any items from it that they wish.

The DVLA and HMRC are clearly incapable of properly handling personal information and should be forbidden from storing or transferring it electronically.

Question 6.

Comments: Providers of Internet services are now required by law to collect a large amount of personal information so that it will be available to the government on demand. I believe that this is a ridiculous and unfair demand on private businesses which have no interest in collecting such information, and for whom it is very costly.

Credit rating companies collect large amounts of information on all users of bank accounts with overdrafts, credit cards, loans and mortgages which is available to almost anyone for a small fee. I believe that this is unfair and that users should have the right to expunge their credit history at any time.

Internet advertising companies, now including Amazon and Facebook which collect advertising data for their own internal use, hold a great deal of information about users which is somewhat scary. So is Google's search database.

Question 7.

Comments:

Question 8.

Comments: Google's search records database is too, and combined with their purchase of Doubleclick gives them much more personal information. I don't believe that regulations on transfer of data between companies provide sufficient protection in the case of such acquisitions, since Doubleclick users never agreed to their data being collected at all, let alone used by Google.

Section 3: The legal framework

Question 9.

Comments: How personal data will be used should be explicitly stated before its entry is required, and a record of explicit consent should be required by law. Inability to prove that consent was given should be grounds for prosecution.

It is unclear to what extent the DPA applies to non-European companies and their activities with respect to European consumers, such as American companies collecting Internet search and advertisement data on British citizens without their consent.

The DPA has no provision to allow users to delete any collected information unless it is erroneous. Factually correct information may still be damaging.

Users should have the right to delete any records held on them (although the company may record such deletion as a new record) and should be able to prosecute companies which fail to comply.

It is difficult for companies to comply with the DPA because they are not always given the opportunity to tell users how their data will be used. For example, on the Internet, mail servers cannot tell you for how long they will store copies of your mail or who they will send it to. This is a technical limitation, but if it was required by law then a solution would be found.

Many companies do not provide any way to opt out of collection of personal information. The DPA does not provide any way to trace where the information came from. As a result I cannot track down the source of all the junk mail I receive, and probably could not stop it even if I did.

It should be possible for users to revoke the permission of an organisation to share their data, in which case the organisation must contact any other to which it has passed the data and inform them that the permission to use it is revoked and they must inform any fourth parties, and so on. Continued use of data after permission is revoked should be a crime.

Question 10.

Comments: Public authorities do not explicitly inform us when our data will be put to new use, e.g. the use of speed camera numberplate records for tracing criminals. The law is made, but not a public announcement, which is left to the media.

Private companies generally obey the letter of the law but not the spirit.

No amount of regulation will prevent data loss and theft.

Question 11.

Comments:

Question 12.

Comments: See my answer to question 9.

Question 13.

Comments: Airlines are now required to provide travel information to the US TSA for flights into or through the USA, although that was illegal under previous law.

The status of banks and other organisations that internally transfer information across UK/EU borders is still unclear.

Question 14.

Comments: There should be the option to opt out of (a) government data collection (since there is no private sector alternative to choose from); (b) data sharing between government departments; (c) governments giving data to the private sector.

The identity card and all use of biometric and genetic information should be optional.

Strong encryption should be required whenever storing or transferring electronic records.

Question 15.

Comments: Data retention laws for ISPs (see above).

Section 4: Consent and transparency

Question 16.

Comments: I believe it is clear in the DPA, but that consumers either do not understand or do not care about their rights, or are willing to sell their privacy.

I have consented to the publication of medical research findings based on information that I have provided and experiments that I have participated in.

Question 17.

Comments: A requirement for consent would impose additional costs on businesses, but I believe that these are reasonable in the circumstances.

Question 18.

Comments: Allow users to trace back where their data came from.

The "reasonable" fee for data access is sometimes very high. Data could be made available online at no cost in many cases.

Question 19.

Comments: I was not aware of the code of practice before, but I believe that it is helpful to have, and that some organisations will improve their data handling as a result.

However I believe that the organisations that we have most to fear from in terms of our privacy, especially large private financial companies, will not change their practices as a result of the code of practice and will continue to just barely comply with the letter of the law.

I think the impact of PIAs remains to be seen in how many organisations conduct them and whether they feel that the expense is justified.

Section 5: Technology

Question 20.

Comments: Sharing information has become several orders of magnitude easier. Thousands of box files fit on a hard disk or a CD; names and addresses of a million people can be matched between databases in seconds instead of months. Information sharing within organisations is taken for granted and essential in modern business.

Electronic theft of data is correspondingly easier, and electronic security is poorly understood and implemented in comparison to physical security. Electronic data theft and loss happens all the time.

As storage capacity increases and more and more data is stored digitally, databases are combined into larger, more dangerous aggregations which make more attractive targets for abuse and theft.

The general public has lost all interest in privacy due to its constant erosion, outright purchase, perceived benefits of its loss, outright lies and exaggerations about terrorism and law enforcement needs and the capabilities of terrorists, lack of technical knowledge, and perceived inability to do anything to prevent it.

Question 21.

Comments: Sensitive personal data should be encrypted wherever it is stored and transmitted, and failure to do so should be treated as either negligence or attempted theft. Only authorised individuals should have access to the keys necessary to decrypt the data and re-encrypt it for a different recipient or use for a different purpose. The key that was used to decrypt the data should be recorded with the decrypted data.

Systems which hold personal data should under no circumstances be physically connected to the Internet, the telephone network or any other network which does not have a physical security perimeter and access control.

Before transferring data between storage devices or systems, the identity of both parties should be established by strong security (tamper-proof physical devices) and recorded on both sides in tamper-proof logs.

The particular standard used for encryption should probably not be specified as it may quickly become obsolete, but it should be of a standard where the Government is confident that it could not crack the code itself. If the encryption mechanism is subsequently breached, all data protected by it should be re-encrypted using a new and stronger mechanism as quickly as possible, and in any case within 6 months.

Question 22.

Comments: Privacy enhancing techniques are very important for data security. For example, under the encryption scheme described above, different columns of the same table could be encrypted with different keys, which allows them to be compared for equality without revealing their actual contents.

This should not just be applied to medical research but to all government records and the private sector should be encouraged to do the same.

Such systems currently require a great deal of technical skill to implement because they are not standardised. Perhaps the government could sponsor or promote the development of free, open source secure databases that could assist with the implementation of such systems at no extra cost to businesses.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments: The USA appears to have a very permissive approach to data sharing combined with stronger individual rights to free speech and privacy. I'm not sure whether they have more privacy or less as a result. Especially the local impact of government terror-mongering makes it difficult to assess whether people are really more ready to share data with and within the government or not. They also appear to have more privacy advocates than we do.

Question 26.

Comments: Countries where the public are especially terrorised by the government and the media appear to have the most public acceptance for loss of privacy, including the USA, the UK and Israel. Citizens of totalitarian regimes such as China, Burma, North Korea, Iran and Saudi Arabia appear to be resigned to government intrusion into their lives. One may argue that the difference between the two groups is less than it appears at first sight.

Section 7: Additional questions

Question 27.

Comments: Whether it is lawful for the government or private companies to use false pretences, such as the threat of terrorism, to justify the creation of new databases, integration of existing databases, and storage and sharing of new information, such as that required by identity cards and passports with biometrics.

Whether data retention laws and government surveillance powers (such as the RIP act) are an undue threat to privacy and burden on individuals and businesses.

Question 28.

Comments: Thank you for taking the time to conduct this review. I sincerely hope that it is useful and that the conclusions are widely and loudly disseminated. I wish you much luck in persuading the media, the government and the public that they should actually care about privacy rather than whitewashing the issue.

I hope that the government, companies and the public can soon be convinced that there is NO WAY to properly protect personal data once it is collected, and that the best protection for its citizens, and for itself against scandal, is not to collect the data in the first place.