

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: My Company been involved in securing data for over 30 years and I have authored security books, articles and features as well as presenting on security issues at numerous events

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

Question 2.

Comments:

Question 3.

Comments: A)loss of personal details to criminals, identity theft, misuse and abuse of personal details held by organisations particularly government and NGO, wrongly collated or incorrectly entered details on one database being carried over affect other databases, with potentially wide ranging consequences A clear example of this has been the experience in the USA where failures of the system (repeatedly denied by the authorities and the system providers (but widely documented) have led to imprisonment of innocent individuals for crimes that they did not commit but which were allocated incorrectly to their ID

numbers or in some cases there were duplication of ID numbers. misuse of information provided to one agency for one purpose and accessed by another. Complete absence of any direction or strategy for use and protection of information which means that information provided or collected today can be used in the future without control of its use. Lack of security or security culture regarding the value of and critical importance of protecting data - witness the HMRC debacle, loss of patient records (and the critical flaws in the NHS system that have yet to come to light). risks for future misuse of DNA information not only for criminal purposes but also for insurance and other medical purposes. This is a small subset of the potential risks of data aggregation with multiple sources of access with or without a strategy and culture for security. And in the absence of individual rights through something akin to a constitution.

b the risks to society in addition to some of those contained above also include the breakdown in trust between the individual and the state that multiple breaches of personal data security will bring about as well as a break down in trust in usage of the structures associated with the Internet. Other risks are that a structured break in to data security systems (for example a breach of the security surrounding biometric data where it would then be possible to substitute different credentials which would then appear valid) would destroy faith in the key single edifice on which these systems are built. Trust in the government as individuals realise the extent to which considerable volumes of centralised data is available to numerous and in many cases only peripherally interested agencies the trust between the individual and the veru institutions upon which society is founded will be damaged (for example we have only to look at some of the errors carried out by social services based on incorrect or misunderstood medical information in regards to children as a fraction of the problem to come).

Question 4.

Comments: some of the scope and methods that carry the greatest risks are those where in the interests of cost cutting or of dogma information is juxtapositioned next to other individual data where it has not relationship and where the provision (often legislatively required) does not justify its use for another completely different purpose.the accumulation of information and connection of that information without any statutory security (or indeed in many cases logical security or even a culture and approach to security as fundamental not peripheral).

Question 5.

Comments: The NHS spine is a good example - this is an interesting and laudable concept carried out in a rush where security has been an afterthought, where the structure of that security means that if you can access the spine with the correct authorisation (and where there are numerous not security aware individuals able to provide that authorisation), or indeed break in, or purchase stolen records you are able to access what once used to be highly secure, strongly protected (and held in only small data sets) personal information which could damage the lives of tens of thousands of individuals for example HIV, mentally ill, immigrants, children, those with predisposition to various genetic factors etc

Question 6.

Comments: An easy example of where the failure in attitude and therefore the failure to legislate correctly to protect data is in supermarkets where they are allowed to collect and aggregate and swap large amount of personal data without any rights as to what that data might be used for. For example joining unhealthy eating habits with excessive alcohol purchasing would make it easy for supermarkets who sell insurance and or finance products to discriminate against those customers that they consider a bad risk. Refusal of insurance is a notifiable situation when requesting insurance elsewhere so individuals may find themselves black listed merely by having for example a Tesco loyalty card and without any means of redress

Question 7.

Comments:

Question 8.

Comments: there are already to many to go through for an exhaustive list

Section 3: The legal framework

Question 9.

Comments: The DPA has been a toothless tiger with the DP commissioner continuing to give both government national and local as well as large industry considerable leeway with minimal prosecution (and therefore attention for) significant, extremely worrying breaches. It is impossible to believe that the DPA has not forced even simple security features such as strong authentication or data encryption on organisations and dealt severely with those who have lost data and haven't even used these. We are dependant for security in enterprise on the requirements of the PCI (payment card industry) to deliver some degree of security requirement around key personal data. The DPA is forced through lack of resources and government will to carry the can for an absence of a proper strategy for data protection (both personal and corporate) in a world where increasingly data is the item with the greatest value. In addition the failure to focus on this area also means that it is possible to circumvent the regulations by outsourcing responsibility or even passing the data outside the jurisdiction. Clearly it is a nonsense to build a data security environment building on foundations of sand and without the government will to consider breaches as merely an embarrassment in their greater goal of ID cards (one merely has to see the absence of any self awareness in their continued pronouncements that they are continuing to this goal)_

Question 10.

Comments: see above. While it is true that some public and some private institutions are aware of and do focus on the limited remit given to the DPA it is under resourced and has no weight - witness the unwillingness of gov in many cases to provide data under the freedom of information act.

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments: This whole section starts from the wrong perspective. If an individual is unable to prevent a statutory authority demanding information, and has no control over what other statutory bodies can be provided with formal access to it (either now or in the future) then standards of sharing information are of no good to him

Question 17.

Comments:

Question 18.

Comments:

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments: technology has made easily available to means to access and copy undreamt of volumes of data and leave no (or minimal) trace

Question 21.

Comments: Should there be legislation - yes. Should it be focussed just on encryption no (and by the way this current government has made it an imprisonable offence to be unable to provide (even if you have genuinely forgotten) access to encrypted data held on your PC, laptop or server). A genuine focus on the value of data to us as a nation, and individuals. with a genuine debate with adequate and balanced representation from all interested parties, which also implies providing balanced funding for those who may represent opposing views to Large industry and the gov.

Question 22.

Comments: a yes anonymisation would help assuming that it was correctly done and some of the current techniques may not achieve that. While advise isn't widely available the biggest drawback is lack of will, for example anonymised data in many cases is of less value to the gov or private industry (for example pharmaceutical companies than granular information)

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:
