

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:

I am interested in the way government and its agencies intends to share personal information, including biometrics, in connection with the National Identity Register but my comments also apply to the sharing of personal information in a more general sense. My response to your consultation reflects the concerns I have in what I think is an extreme example of proposed data sharing, but one that encapsulates the debate. I do not have any other connection with the collection or sharing of personal information - other than being a 'data source'.

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

Question 2.

Comments:

While there are advantages to individuals of sharing information I leave it to others to comment on these. I am more concerned with the advantages to government of the proposed NIR and its motives for setting it up. Having personal information freely exchangeable between government departments and

agencies (etc) makes it easier to control society by controlling the individuals - to what end is unclear but raising taxes, limiting individual freedom, and influencing behaviour in any number of ways are obvious candidates. The reasons given in support of the NIR are hopelessly inadequate and do not stand up to any form of close scrutiny - but this is not the place to go into them.

Question 3.

Comments:

A principal risk of the sharing of data is the potential for abuse of the system by the very large number of people who will have access to details of our private lives and activities. We do not know who they are but they will include police, tax officials, social security staff, customs and excise and other minions of the state too numerous to mention. I know people in these roles and very few of them are paragons of virtue, above suspicion, who would never abuse the access they have. An example of such 'abuse' is the police officers using the police national computer to identify the owners of cars whose alarms are going off outside their houses. It is not what the system was designed for and if ordinary members of the public wanted such information it would (rightly) be denied. But an officer of my acquaintance has told me that he has done just this on several occasions. A minor example, but one which could have more serious consequences if the motive was different or the information on the database was more personal or sensitive in any number of ways.

Another less definable, though potentially more pervasive risk is the potential for government to interfere with our lives through the ability to analyse data gathered for a variety of unconnected reasons. The temptation to do things 'because we can' will be irresistible to some. The NIR will give an ideal opportunity to introduce more restrictions and controls into our lives or, at the very least, burden us with administrative tasks which will be of little or no benefit for individuals, and probably little real use to our masters. Exactly what these may be is difficult to predict, but we can be sure that the law of unintended consequences will have a field day.

There are of course more fantastic possibilities that paint a horrifying vision of the future - the film Brazil and George Orwell's 1984 are obvious examples. I do not have any information that the NIR will be used for such brutal purposes by the state, but once again the fact that it is possible will make it very tempting to some - imagine what fun Mrs Thatcher's more uncontrollable lieutenants would have had with a NIR and ID cards. And none of us know the nature or persuasion of administrations down the road in our children's futures. Let us not give those with a tyrannical bent any more help than is strictly necessary.

Question 4.

Comments:

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

Question 10.

Comments:

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

There will be no question of consent for the NIR, the government will do as it wants with the data whether we like it or not, let alone agree. There is no doubt that the 'voluntary' aspect of it is a temporary arrangement to get the bill through parliament and that in all practical terms, and the intention is that, to operate at any reasonable level in the UK (i.e. not be a non-person) an ID card will quickly become compulsory.

Question 17.

Comments:

Question 18.

Comments:

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments: There are two significant technical advances that have made the NIR possible - i.e things that would rule out a paper based system. Firstly it is possible to record and process an individual's biometrics digitally. This allows unique personal details to be used as the main means of identification of individuals on database. Once the security of this information is compromised, as it surely will be for some if not all of us, it is impossible to issue an alternative. We are who we are and we cannot change out iris patterns, fingerprints or DNA. The second significant technical advance is the ability to copy and pass information networks both wired and wireless. This makes the transmission of data fast and ubiquitous - it will be available to any official with the right equipment anywhere in the UK and beyond.

Add to this the government's inability to reliably commission and operate large data systems and we have a recipe for disaster - with any luck it will only be financial.

Question 21.

Comments:

There must be a requirement to protect data, not only by encryption but also those individuals who have access to it. The problem is that the 'digital information age' is in its infancy, we do not have the need for security ingrained - I know several people working at various levels of administration in our offices of state who cannot use a computer, and are proud of it, they would be unemployable if they couldn't use a phone or a pencil (disability issues notwithstanding). We have not reached a stage where the protection of data is second nature as it is with, for example our children, cars and money. The systems used for storing and transporting sensitive data are still being developed, often it seems by individuals based on very poor understanding of how the world works. For example it is difficult to credit that HMRC copies large amounts of data onto CDs and couriers them to the US for processing, or that military personnel, officers of hospitals, banks and other financial institutions are able to keep laptops loaded with unencrypted data in their cars. Imagine the data was gold bullion, it just would not be 'allowed'. We do not, as a society, have enough experience of data security to trust our irreplaceable data to large shared databases. It's a data Titanic with fire doors open, one breach and the whole lot is compromised.

Question 22.

Comments:

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: FYI: This form is quite difficult to use (selction of text and moving between questions is difficult). Also there are no questions (see above) on the copy I downloaded - I had to refer to the consultation document to find out what the qustions were. To some extent this illustrates my point above about not really having assimilated computer technology - documents sent out for consultation should be better thought out and easier to use - but we are all still learning how to use this 'new' technology.
