

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 Experience

I have 15 years experience in data sharing development.

I am Managing Consultant of Financial Information Markets, specialising in consulting on data sharing across the private and public sectors. I have most recently been involved in lobbying on the course of the data sharing provisions of the Serious Crime Act 2007. Previously I worked for LTSB, and represented their interests in this field at the BBA, FLA etc.

I wrote and negotiated the 'Principles of Reciprocity' which govern the credit and related data sharing of the 500 or so UK retail companies involved, and was a chairman of SCOR, the governance committee. I was also chairman of Insurance Database Services Ltd, and founded the Insurance Fraud Bureau.

The data sharing

Many of my answers to your questions below draw on my experience with 1 the credit and related data sharing schemes, and 2 The Insurance Fraud Bureau. 3 I will also draw on my experience of working on the data sharing provisions of the Serious Crime Act 2007 for some later questions.

1 I will assume you are well aware of the extent and arrangements for the credit and related data sharing scheme.

2 The Insurance Fraud Bureau is a secondary use of data: it merges information from the Motor Insurers Database, the Claims and Underwriting Exchange and the MIAFTR motor fraud investigations database. Together these provide nearly all the shared information available on the insurance industry's history of general insurance claims and records of motor insurance. The combined database is then analysed for evidence of networks of serious and organised crime activity, and cases investigated by priority of severity. I am involved in original research using the database at present.

3 The Serious Crime Act 2007 will provide for the development of public – private sector data sharing for fraud prevention and control.

Note – The questionnaire and the review is entitled, correctly in my view, the Data Sharing Review. It then often refers to information rather than data. I prefer to stick with data in my responses, as in my view it is generally data which is actually shared, which is then turned into information subsequently – that is often the purpose of the sharing.

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

Question 2.

Comments:

a)

1 The benefits to individuals in sharing credit and related data show in the easy access of UK subjects to credit and related products, and to the effectiveness of the remote verification of identity. The forms of credit assessment that rely on data sharing such as credit application scoring and behavioural scoring have been shown to be far less likely to discriminate for example on the grounds of race or gender than the previous traditional personal assessments made by senior branch staff.

2 The benefits to individuals from an initiative such as the Insurance Fraud Bureau come in the reduction of overall fraud and hence shared cost of insurance. They also come for example more immediately in the likely reduction in staged accidents – a pernicious form of fraud where innocent members of the public have been victims.

b)

1 Society benefits from the wider availability of credit in the form of increased GDP and greater opportunities for individuals. The World Bank has recently assessed this UK data sharing scheme as providing major economic benefit to the UK consumer sector.

2 Society will benefit from initiatives such as the Insurance Fraud Bureau by the ability to oppose the growth of organised crime.

Question 3.

Comments:

a)

1 The risks involved for individuals in the shared credit and related data scheme include a steady potential widening of the scheme to include organisations and sectors beyond traditional credit, and in the value the information provides, for example for identity. It also has some potential for use against the spirit of the rules in marketing rather than credit.

2 So long as the Insurance Fraud Bureau data is kept secure (and security arrangements are excellent), there seems little potential risk to the majority of UK individuals. It is always possible that innocent persons will be caught up in fraud, and indeed deliberately targeted, but the risks associated here to them in any action taken against fraud from this information sharing look to be no different from any other form of action against fraud.

b)

1 That there are many risks to society in the operation of readily available credit seems very obvious in the wake of Northern Rock, and the recent Egg account closures. But I would say that these risks are to do with incompetent credit management, and not information sharing per se.

1 I would say that risks from information sharing to society as an aggregation of individuals are more likely to be related to weaknesses in governance.

2 The Insurance Fraud Bureau scheme is so specialised that it is hard to think of anything other than an aggregate benefit to society.

Indeed there are some societal advantages in this field over non-data sharing across an industry sector: An industry data sharing scheme such as the Insurance Fraud Bureau actually evens out this aspect of risk between different companies, and thus may be looked at askance by some larger companies with better anti-fraud arrangements and economies of scale. Larger companies will also pay more as part of pooled costs: smaller companies benefit dramatically from such arrangements when their cost/benefit ratios are considered. As the individual consumer is unlikely to be able to assess fraud risk in advance of choosing insurance from any particular company this may also be a benefit, and over and above the competitive smoothing such schemes may represent.

Question 4.

Comments:

On scope,

in general terms the more complex and wider the scope of information sharing, the greater the opportunity for value exploitation, as personal data is per se of considerable value in aggregate. That brings greater risks in terms of breaches of the spirit and terms of the data protection act and the consumer protection it represents. That implies that data sharing scheme governance needs to be more effective as scope becomes more complex and wider. It also implies, all other factors being equal, that regulation might be more focused in such areas.

On methods,

there seems by publicised experience to be a clear distinction between well established data sharing schemes run by intermediary specialised data sharing companies (such as Experian, Equifax, Call Credit, Symantec, Detica) and ad hoc arrangements however large their scale or potential impact. (This point applies especially to the public sector but also to the private sector.)

Such companies typically pay very close attention to data security including security of transportation, not least because of the commercial hazard they would face if there were major failure. Such companies are in addition specialised in data transmission and handling by their very nature – cross company data sharing in the private sector is typically mediated by such specialised companies, whereas such development seems far more uneven in the

public sector.

I believe that these specialised companies quoted above are exemplars here, and the following comments refer to the ad hoc arrangements I refer to above.

The steady developments in data handling technology at individual level (such as portable PCs, writeable CDs and DVDs, memory sticks, portable hard drives) mean that ever larger volumes of personal data may be transported by single individuals and potentially lost.

The fault, I would say, remains fundamentally with the organisation that is responsible for the data in the first place. Personal data should be available for individual download only under highly secure circumstances, and encryption should be standard.

Individuals should be adequately trained in the implications of the data protection act, and in the workings of risk and impact assessments, and face sufficient sanctions for failure to protect the security of such information.

Typically, untrained individuals have only the most amateur ways of assessing risk, and fail to take impact into account and its interaction with risk. A basic risk and impact assessment will multiply risk and impact. Untrained individuals will also not understand the importance and requirements of the Data Protection Act 98 and related legislation.

Question 5.

Comments:

3 Here I will refer to my experience with the provisions of the Serious Crime Act 2007.

There is great scope for data sharing between the public and private sector, and especially on the field of fraud. Fraudsters do not need to distinguish between public and private sector, and the two sectors are thus at a substantial disadvantage unless they do collaborate in this way.

I am not providing a view on whether the public sector is holding too much data as this is outside my experience.

Question 6.

Comments:

As for my answer in Q5 above, there is great scope for data sharing between the public and private sectors, especially in the field of fraud.

See my answer to Q8 on whether private sector data sharing schemes hold or provide too much data – I am not providing a view on whether private sector organisations per se hold too much personal data.

Question 7.

Comments:

Comprehensive data sharing on the model of the Insurance Fraud Bureau would be appropriate and valuable amongst banks, but is not currently under development, though a number of less ambitious schemes which directly share reported fraud are under development.

I can answer the second part of the question on what are the barriers to be overcome to share data which is clearly in both public and commercial interest from my experience in founding the Insurance Fraud Bureau. I and the data sharing body I chaired did overcome those barriers, but they were in aggregate quite formidable.

While the legal position is complex, regulators provided highly approachable support – we kept the IOC informed from an early stage. Government in the form of SOCA also proved encouraging and helpful. Cultural barriers can be addressed by leadership and using press and industry bodies. Starting from an existing specialised industry data sharing company allowed a vehicle for start-up funding. Institutional barriers were very challenging, but again an industry company structure plus the trade association body, the ABI in this case, allowed these to be engaged successfully.

Question 8.

Comments:

Whether or not private sector data sharing schemes hold too much data depends on a view on the agreed objectives of those schemes, customer notification, understanding, and tolerance of those objectives plus a view arising from regulation as to what is necessary for the stated purposes. 'Mission creep' is possible where data shared is highly valuable, suitable for a wider number of purposes than originally intended, and governance does not fully represent all of the stakeholders involved.

The risk of 'mission creep' is that information sharing can develop a life of its own led by the value of the information shared rather than the starting objectives. It may also develop beyond consumer comprehension of the purpose of information sharing, becoming something complex, incomprehensible and tolerated rather than positively understood and accepted.

In particular, individual customers in aggregate as providers of data as well as consumers of the services it is used to support are insufficiently represented organisationally.

In this context, a benign development is the increasing ability of consumers to access their own credit records – for example Credit Expert provided by Experian has proved highly popular with a very wide range of consumers, not just those attempting to understand why they were refused a particular line of credit.

Section 3: The legal framework

Question 9.

Comments:

On the whole the DPA works well as a legal framework, and the principles have the advantage of being in plain language and comprehensible.

It seems most unlikely however that more than a very small minority has a grasp of even these, and thus 'data protection' is open to all sorts of popular misinterpretations.

Some data protection training should be available to the population at large, perhaps during schooling – just a basic amount would make a major difference I believe.

The IOC is arguably under-resourced, and I would support Richard Thomas' views on the need for active audit powers. I would also expect that active audit would be to the advantage of the specialist data sharing companies, though that is a case for them to make.

I would also support criminal sanctions to deal with data trafficking.

The DP Act 98 does not deal with data sharing as such, for example there are no terms relating to sharing overtly or to its governance. There is a framework of controllers and

processors as well as third parties that can be applied, but looks as if it was designed for a model where processing is carried out mostly by a single company and potentially agents working on its behalf.

The ICO Framework code for sharing information is useful, as is the requirement for public sector bodies to agree an acceptable code, I suggest there should also be standards relating to the governance bodies of information sharing, say when more than just 2 sharers are involved.

Such information sharing schemes can be very complex and dynamic in terms of their development – they should be comprehensible to the data subject as entities in their own right, not just on the occasion of an item of processing that affects them, as if they were no more than an aspect of processing by a single company. The data subject should be able to deal with them as a single entity, and not just be forced to follow a trail of items of their data passed from one processor to another.

Responsibility and liability should also be clearly assigned – the data subject is likely to be confronted with a complex audit trail if they attempt to track where items have come from. While a certain level of confidentiality may be appropriate in some areas, such as fraud, in general there are strong arguments for far greater transparency here.

There is a practical balance to be kept between the operation of the Act and the individual protection it represents, and the continued development of data sharing and other forms of use of personal data. I believe the balance is much better in the UK than in some other European countries, where such development has been far more restricted by differing interpretation and implementation of the same data protection directives.

Question 10.

Comments:

Question 11.

Comments:

See my answer to Q9 paras 1,2,3

“On the whole the DPA works well as a legal framework, and the principles have the advantage of being in plain language and comprehensible.

It seems most unlikely however that more than a very small minority has a grasp of even these, and thus ‘data protection’ is open to all sorts of popular misinterpretations.

Some data protection training should be available to the population at large, perhaps during schooling – just a basic amount would make a major difference I believe.”

Question 12.

Comments:

See my answer to Q9 paras 4 5

“The IOC is arguably under-resourced, and I would support Richard Thomas’ views on the need for active audit powers. I would also expect that open audit would be to the advantage of the specialist data sharing companies, though that is a case for them to make.

I would also support criminal sanctions to deal with data trafficking.”

And to Q9 paras 6 7 8 9

Question 13.

Comments:

Question 14.

As for Q9 para 5

“I would also support criminal sanctions to deal with data trafficking.”

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments:

See my answer to Q9 paras 6 7 8 9

Question 19.

Comments:

See my answer to Q9 paras 7 8 9

“While the ICO Framework code for sharing information is useful, as is the requirement for public sector bodies to agree an acceptable code, I suggest there should be standards relating to the governance bodies of information sharing, say when more than just 2 sharers are involved.

Such information sharing schemes can be very complex and dynamic in terms of their development – they should be comprehensible to the data subject as entities in their own right, not just on the occasion of an item of processing that affects them, as if they were no more than an aspect of processing by a single company. The data subject should be able to deal with them as a single entity, and not just be forced to follow a trail of items of their data passed from one processor to another.

Responsibility and liability should also be clearly assigned – the data subject is likely to be confronted with a complex audit trail if they attempt to track where items have come from. While a certain level of confidentiality may be appropriate in some areas, such as fraud, in general there are strong arguments for far greater transparency here.”

Section 5: Technology

Question 20.

Comments:

See my answer to Q4 paras 2 3 4 5 6

“there seems by publicised experience to be a clear distinction between well established data sharing schemes run by intermediary specialised data sharing companies (such as Experian, Equifax, Call Credit, Symantec, Detica) and ad hoc arrangements however large their scale or potential impact. (This point applies especially to the public sector but also to the private sector.)

Such companies typically pay very close attention to data security including security of transportation, not least because of the commercial hazard they would face if there were major failure. Such companies are in addition specialised in data transmission and handling by their very nature – cross company data sharing in the private sector is typically mediated by such specialised companies, whereas such development seems far more uneven in the public sector.

I believe that these specialised companies quoted above are exemplars here, and the following comments refer to the ad hoc arrangements I refer to above.

The steady developments in data handling technology at individual level (such as portable

PCs, writeable CDs and DVDs, memory sticks, portable hard drives) mean that ever larger volumes of personal data may be transported by single individuals and potentially lost.

The fault, I would say, remains fundamentally with the organisation that is responsible for the data in the first place. Personal data should be available for individual download only under highly secure circumstances, and encryption should be standard.”

Question 21.

Comments:

In general terms the law should do so, though being careful to avoid criminalising innocent and unavoidable personal use, such as address books.

Question 22.

Comments:

I cannot say I have sufficient expertise here, though in my personal experience either depersonalisation places an unacceptable limitation on the usefulness of research, or else is in practice very hard to actually achieve. I believe the answer is to adequately protect personal data in its full form.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

As I have said in answer to earlier questions, and from my personal experience with complex and very wide ranging information sharing, I would like to see any future iteration of the Data Protection Act take a fuller account of information sharing, rather than just provide a data processing and control framework to be applied. While I welcome the framework code of data sharing, in practice the more large scale and complex an information sharing scheme becomes, the more it is likely to need some form of active governance, and not just adherence to a code. I have said in connection with this point that individuals are under-represented as stakeholders in much complex information sharing, though there are developments (such as Credit Expert by Experian) that will allow them to develop a sense of knowledge and ownership over what is after all their data.

Question 28.

Comments: