

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:

Equifax, one of the leading credit assessment, ID verification and fraud prevention solution providers, is delighted to respond to the Data Sharing Review being led by the Information Commissioner, Richard Thomas, and Dr Mark Walport, Chair of the Wellcome Trust.

Equifax in the UK was established in 1989 and now has over 520 employees across sites in London, Bradford and Wexford. We serve customers across a wide range of industries including financial services, retail, healthcare, telecommunications/utilities, brokerage, insurance and Government departments.

Originally established in the USA in 1899, we are headquartered in Atlanta, Georgia, and employ approximately 6,900 people in 14 countries through North America, Latin America and Europe. Equifax is a member of Standard & Poor's (S&P) 500® Index.

We are the world's largest repository for consumer credit information, and in the UK we hold approximately 400 million records on 45 million individuals. We receive in the region of 192 million updates to this information each month from financial, telecommunications, retail and other sectors. Our commercial databases contain information on 2.1 million limited

companies as well as information on a significant number of non-limited companies.

The data we hold is collected from a range of public and private sources including Government bodies such as Local Authorities (Electoral Roll), HM Court Services (via Registry Trust Ltd) and organizations involved in granting credit, including all the banks, credit card companies, mortgage providers, mobile telecommunication providers and mail order companies.

Our services and systems are structured around compliance. Customers are vetted and can only access the product they are eligible for. Contracts with customers clearly set out the terms and conditions for access. Access to these products is tightly controlled through the use of account numbers and passwords.

We use this data to provide services to business, individuals and Government. In particular we offer:

- consumer and business credit intelligence
- portfolio management
- ID verification and fraud prevention
- decision-making technology
- marketing tools

Our business model is based on secure, accurate data. As such, we invest heavily to ensure that our databases and business processes are in line with the principles of the Data Protection Act (DPA). In the UK we have received accreditation to the Government T Scheme, as well as BS 7791 and ISO 27001 which means our processes are defined, documented and checked every year.

Our staff under go continuous training to ensure they are aware of their responsibilities, and we have set in place a number of checks and measures to ensure that all database activity is monitored and assessed to ensure appropriate use.

Our clients only have access to allocated products, and, importantly, no external organisation or individual is provided with direct access to our databases. Furthermore, all requests are monitored, and individual records are marked with a 'footprint' every time they are accessed to allow us to monitor activity effectively.

The Review may be particularly interested to note that Equifax's global information security policies are based on our UK model.

We believe our services make a real contribution to businesses, individuals and increasingly Government.

The following document outlines our experiences of information security in the UK, and how information sharing can be enhanced to help provide the best possible services across the public and private sectors. In particular, we would like to highlight the following key themes which arise from this document:

1. We believe that the DPA provides an effective framework to protect information in the

- UK, and allow for effective data sharing
2. However, greater clarification and guidance from the Information Commissioner would prevent misinterpretations of the Act and allow for easier implementation by public and private sector organisations
 3. There needs to be greater awareness by individuals, business and Government of the need to protect personal data and ensure its appropriate use

We would be delighted to meet with the Review Team to discuss this document and our work in greater detail.

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

Question 2.

Comments:

Both the private and public sectors rely on accurate data in order to conduct the everyday activities we have come to expect and rely upon as individual citizens.

In the commercial sector, data is used by banks and retailers to assess risk when lending to individuals and businesses. This is an essential part of their business process, and is key to ensuring that individuals are able to take advantage of the services provided by lenders in the UK.

Sharing personal information also allows organisations to understand borrowing habits, and therefore lend responsibly, reducing the likelihood of over indebtedness.

Data sharing also creates greater choice for the consumer. Traditionally, in industries such as the financial sector, only an individual's bank would be able to assess lending risk to that customer. Secure technologies now allow organisations such as Equifax to provide financial institutions with the information they require quickly and accurately to assess the risk posed by a potential customer. This improves customer service, and allows banks to compete for customers.

The public sector is beginning to benefit from effective data sharing. Working alongside Government departments and other public sector bodies including the Identity and Passport Service (IPS), HM Court Services and the Department of Work and Pensions (DWP) we are helping the public sector take advantage of data sharing to combat fraud and help to trace individuals who owe money.

Question 3.

Comments:

As outlined at the beginning of this submission, we believe that the DPA provides an effective framework for the protection of personal information.

However, without clarification from the Information Commissioner on the implementation of

this legislation, there will always be organisations that fall foul of the DPA's principles, either by accident or design. It is where organisations are unaware of their obligation under the DPA, or disregard this legislation, that the greatest risk of sharing personal information lays.

Equifax has worked hard over the last decade to ensure we have one of the most secure information systems in the world. We have achieved this by developing systems which place the principles of the DPA at the centre of all our activities.

It should be noted that Equifax has the resource to make this investment in meeting the principles of the DPA. Many organisations, in particular small businesses, have neither the time nor money to make this investment. We believe that clear guidance and support from the Information Commissioner would ease the implementation of the DPA's principles, and ensure that all organisations can do their utmost to protect personal information.

Question 4.

Comments:

We believe that the greatest opportunities to benefit from data sharing arise when an individual has the ability to understand how their data is used and protected. This understanding helps to create an open and transparent environment, in which consumers are comfortable with the availability of their personal data, and businesses are able to rely on the information they receive.

The greatest risks therefore arise in an environment where there is a lack of transparency creating distrust and suspicion of business practices and the information which is collected on individuals.

A key part of this approach is proportionate processing. At Equifax, our systems ensure that we only share the data an organisation may require to complete their business processes. Responding to an information request with all the information we hold on an individual would be both disproportionate and irresponsible.

We believe that the Information Commissioner should issue clear guidance, which will encourage transparent working practices and ensure that businesses and consumers have an understanding of their rights and responsibilities.

Privacy Impact Assessments (PIAs) are a step towards this approach, and will assist businesses in developing new products and services. They will also help to increase transparency and openness, engendering greater trust amongst individuals.

Questions 5 and 6.

Comments:

We believe it is not the quantity of available information which should be addressed, but rather the quality of data and openness of the organisations that hold it. Restricting the flow and availability of data has the potential to damage accuracy and usability of personal data – in turn affecting the services which can be offered to individuals.

Equifax holds information on over 400 million individuals which is continually updated and new individuals added. In order to protect these individuals and provide the best possible service to our customers we take a number of steps to ensure that this data is as accurate as possible.

As a part of this process we collect data from a number of sources, and are as open and transparent about our processes as we can be without compromising data security. We actively encourage consumers to check their data files to ensure that the information we store on them is up-to-date.

We believe there should be greater encouragement for individuals to check their data files to ensure that the information held on them is accurate. It should be the responsibility of business and Government to ensure individuals are aware of their rights.

Question 7.

Comments:

Effective data sharing creates a number of opportunities for individuals, as well as for the public and private sectors.

This is particularly the case in the area of financial inclusion where improved data sharing between lenders was identified in 2006 by the Treasury Select Committee as an area which could significantly improve prospects for some borrowers.

As we have stated throughout this response, the key to effective data sharing is transparency and openness. Consumers must be aware of how their information is used, and how they can engage with the organisations which hold data on them to ensure it is up-to-date.

Similarly, organisations must understand the principles of the DPA and how these should be implemented. It is in this environment that data sharing will provide the greatest benefits to individuals, businesses and Government.

Question 8.

Comments:

N/A

Section 3: The legal framework

Question 9.

Comments:

Equifax believes that the DPA offers a strong framework for the protection of personal information. The clear strength of the Act is that it strikes an effective balance between the rights of the individual and the needs of the public and private sectors.

However the principles of the Act are open to interpretation, creating the potential for organisations to take advantage of personal information without fear of being brought to account.

We believe the Information Commissioner should seek to issue more guidance around the principles of the DPA, to clarify the role of data handlers and ensure that organisations are unable to develop their own interpretation of the Act.

This approach should be supported by proactive engagement with organisations and individuals to ensure an understanding of the DPA, individual rights, and the requirements on the public and private sectors.

As we have set out above, there should also be a focus on smaller businesses and organisations, to ensure they have the support to fulfil the principles of the DPA.

Question 10.

Comments:

The second principle of the DPA is fundamental to Equifax's business model, and we have made a significant investment to ensure that we meet the requirements of the DPA.

We have included some information in the document on the processes we have set in place to meet this principle, and would be happy to discuss these in greater detail with the Review team.

Question 11.

Comments:

The biggest barrier which inhibits the effectiveness of the DPA is the lack of resources available to the Information Commissioner, and the public and private sectors.

The Information Commissioner's Office (ICO) should be given appropriate resources to allow it to develop relevant guidance, and ensure that the Information Commissioner has the ability to engage directly with organisations, both to educate them, and to ensure compliance with the Act.

There must also be wider engagement with the public to ensure an understanding of individual rights under the DPA. This would be particularly beneficial as it would lead to greater accuracy of information, and build trust amongst individuals, and an understanding of the importance of information sharing.

Further to this, organisations across the public and private sectors have a responsibility to make the resources available to ensure that they can implement the principles of the DPA, and provide the greatest possible protection for individual data.

It should also be noted that while Equifax recognises and implements the provisions of the DPA, many organisations remain unaware of their responsibilities. Greater guidance and support from the Information Commissioner would help to address this situation.

Question 12.

Comments:

As set out above, we believe that the DPA provides an effective framework for the sharing and protection of information. However, greater clarity is required to ensure that organisations abide by the principles of the Act.

We welcome recent proposals to increase the powers of inspection for the Information Commissioner. In addition, increased penalties for the wilful misuses of personal information would also increase the importance of protecting data, and reduce the opportunity for inaccurate interpretation of the DPA.

Questions 13 and 14.

Comments:

There are a number of pieces of UK legislation which have a positive impact on data sharing and data protection. In particular, we believe that the following Acts provide clarity around specific areas of information sharing and support the principles of the DPA. They include:

- ID Cards Act 2006
- Child Support Act 1992
- Serious Crime Bill 2006
- The Supply of Information (Register of Deaths) Regulations 2007

We do not believe there are any changes to the DPA or further statutory powers that would enable better and more secure sharing of personal information. However, we accept that new technologies, threats and the development of new services may create a requirement for further legislation in the future.

It is vital that any future legislation should reflect the principles of the DPA.

As set out above, the priority should be to develop guidance which will enable individuals and organisations to better understand their roles and responsibilities under the DPA.

Question 15.

Comments:

We do not believe that there is an unreasonable burden on business to comply with the existing legal framework.

However, greater clarification and support from the Information Commissioner, particularly for smaller businesses, would aid efforts to implement adequate information sharing practices.

Section 4: Consent and transparency

Questions 16 and 17.

Comments:

This is an area where greater understanding of the provisions of the DPA would be beneficial. It should be the role of businesses, Government and the regulator to ensure that consumers are aware of their rights under the DPA to see information held on them.

Section 7 of the DPA clearly sets out the circumstances under which consent is required for the sharing of an individual's data.

We believe that this Section of the legislation currently provides adequate safeguards to ensure sufficient transparency and protections for consumers.

This is supported by the rights of every individual to request information held on them by an organisation.

Further to this we have developed our own systems to provide a further level of transparency. Equifax ensures that individuals' files are marked with a 'footprint' each time a request is made to review the information held on them by an organisation. We provide this information on request, allowing individuals to keep track of exactly which organisations have accessed their data.

Question 18.

Comments:

Equifax fully supports an individual's right to access information held about them. Section 7 of the DPA secures this right, and we believe that this section of the legislation currently provides adequate safeguards to ensure sufficient transparency and protections for consumers.

These rights are essential to building trust and it should be the role of businesses, Government and the regulator to ensure that consumers are aware of their rights under the DPA to see information held on them.

The credit and lending industries have undertaken a number of initiatives following the implementation of the DPA to ensure that consumers are aware of their rights under the legislation.

In particular, the Banking Code provides a voluntary code of best practice for financial institutions to follow when dealing with personal customers. The code includes a section on personal information which sets out that those institutions which have signed up to the code will explain to customers that under the DPA they have the right to see the personal records held about them.

The latest edition of the Banking Code can be accessed online here, and is expected to be updated by the British Bankers Association in March 2008:

<http://www.bankingcode.org.uk/pdfdocs/BANKING%20CODE.pdf>

Further work must be done to educate industry, and particularly small businesses, about the need for appropriate data protection infrastructure. Equifax has invested heavily to ensure that our systems meet the principles of the DPA and our entire approach is based around transparency. Similar investment across industry will build trust amongst individuals that their data is secure and being used appropriately.

To achieve this, clear guidance is required from the Information Commissioner around the principles of the DPA, clarifying organisations' responsibilities under the legislation.

Question 19.

Comments:

We believe that the principles of the DPA provide an effective framework to ensure appropriate transparency, scrutiny and accountability.

Clear guidance and clarification from the Information Commissioner will enhance the principles of the DPA, and ensure that businesses understand their obligations and individuals their rights.

As business needs and offerings change, the Information Commissioner should update this guidance to ensure it is relevant, and continues to provide a clear framework for the protection of personal information.

Section 5: Technology

Questions 20, 21 and 22.

Comments:

Equifax has made a significant investment in information systems to ensure that the data we hold is secure, and can be delivered to clients and individuals quickly and effectively. Technology has played an important part in this process, and we work closely with our outsourced IT partner to ensure that we can continue to provide the best possible level of service and security.

Whilst we are not able to publish information on these systems, our technical experts would be happy to meet with the Review team to discuss how Equifax holds and shares data securely with over 30,000 organisations in the UK.

More generally, the Review may be interested in a recent Demos report, *National Security for the Twenty-First Century*, which commented that relationships between the Government and the public must be based on a set of firm principles for making national security transparent, accessible and accountable for all. The report makes the case for developing a technology platform for sharing information among Whitehall departments, agencies and police based on the success of Intellipedia in the United States.

Intellipedia is an online tool used by the Office of the Director of National Intelligence in the U.S., and allows effective data sharing between a number of intelligence areas. The primary goal of the system is to allow intelligence operatives to join the dots, and gain a wider picture of threats to the country.

The Demos report sets out that, building on the current IT programme SCOPE, Intellipedia would allow information to be shared on a secure platform across Government. The full report from Demos can be accessed online here:

<http://www.demos.co.uk/files/National%20Security%20web.pdf>

Further to this, a debate within the industry has recently begun around the potential for introducing a BS standard on Data Protection. An existing 27002 ISO standard sets out the code of practice for information security. It details hundreds of specific controls which may be applied to secure information and related assets.

Although it is in the early stages, such a BS standard would create a benchmark for information security across business, and provide a clear set of actions for information controllers to follow.

Section 6: International comparisons

Questions 23 and 24.

Comments:

Equifax has invested significantly, in developing effective information security policies and systems over the ten years following the creation of the DPA.

The standards set in place in the UK, were guided by the principles of the DPA, and have led our global information security practices.

Question 25.

Comments:

Equifax is a member of the Association of Consumer Credit Information Suppliers (ACCIS), which brings together 30 consumer credit reference agencies in 22 European countries and associate members from all other continents.

As part of our work in 2007, ACCIS conducted a study into the legislation and commercial activity surrounding data sharing across European countries. This research raised concerns about the future of information sharing internationally. In particular, it demonstrated that 70% of ACCIS members are unable to share information across borders. Essentially if an individual wanted to move from Spain to France and change banks, their new bank in France would not be able to obtain any information on that individual from their previous institution.

This environment will be increasingly restrictive as movement across European borders

grows. It is also detrimental to competition, and has the potential to damage businesses seeking to expand into the European Union area.

Question 26.

Comments:

N/A

Section 7: Additional questions

Questions 27 and 28.

Comments:

N/A