

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: Symantec is the fourth largest software company in the world providing solutions that help individuals and enterprises assure the security, availability, and integrity of their information.

In general the type of personal information which may be collected by providers of IT services and software may include name, address and contact details, such as e-mail addresses, and credit card information for transaction processing. This sort of information is often collected through vendors, in high street stores and possibly on-line. For business customers and enterprise partners contact information is collected and used for contract fulfillment, to enable product and services customisation, and for registration in partner programs, newsletters and possible promotions. However, personal data is only passed onto business partners upon explicit consent of the personal data owner.

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

Question 2.

Comments: The exchange of personal information is necessary for the creation and delivery of almost all goods and services. Commerce could not exist without the exchange of personal information. The sharing and processing of personal information using technology has enabled the development and delivery of efficient, customised and increasingly innovative goods and services by both the public and private sectors. The benefits to individuals and society alike include increased personalisation of goods and services built on customer individual requirements and the ability to gain access to these goods and services quickly and effectively. In Symantec's role as a consumer software vendor, personal information allows us to provide a shopping experience which is personalized and comfortable, and allows subscribers to manage their subscriptions and software easily. It allows Symantec to reach out with offers and products attuned to the needs of our consumers. The information gathered about business contacts makes us more efficient in addressing and understanding the needs of our enterprise customers, and fulfilling them.

For society the benefits as a whole are numerous. The exchange of personal information through technology is enabling the transformation of public service delivery in the UK; a visionary strategy that will improve the quality, efficiency and cost effectiveness of public services. However, for the opportunities of transformational government to be fully realised greater sharing of personal information between and within government departments to develop citizen centric services will be required. The aggregation of personal information will enable organizations to better understand society's needs, concerns, and desires and to respond to them accordingly. However, the take-up by citizens of e-government services will rely on having appropriate systems, processes and safeguards in place that can ensure the confidentiality, integrity, availability and privacy of personal data shared with government.

Question 3.

Comments: Except for those at the extreme end of the scale (privacy adverse individuals who have retreated into bunkers, or those with bedrooms based webcams), most people fall into the category that they are willing to exchange some personal information for a benefit. The problem that may arise though is in honoring the bargain that was made. A key risk to both individuals, and thus to society, is therefore where personal information is used in unexpected or unreasonable ways, for example if information is used for a purpose that was not contemplated or understood by the individual at the time the personal information was collected. Furthermore when personal information is shared with unexpected parties, or is exposed through some data loss.

Citizens fears over how their personal information is being processed, stored, accessed and shared present a major challenge to the future delivery of high-value added goods, both off and online, and public services. Gaining and maintaining the trust and buy-in of citizens that their data is secure and protected will be essential to allay public fears, realise the full benefits and opportunities provided by technology and increase citizen's confidence in the online connected world.

Question 4.

Comments: It is suggested that before determining the opportunities and risks to the current scope of data sharing, further discussion is needed to define what is, and what is not, considered personal information. Once this is clearly defined an assessment as to whether the way information is being shared is proportionate and necessary can be fully determined. Furthermore the risks associated with data sharing should be assessed against the original purpose for which the data was provided, regardless of the method by which the data is being shared.

Clearly today there are many new innovative ways and opportunities for the public to share their personal information. These can include entering personal profile information on a web portal, uploading one's location to a web site with GPS data or even through using social or business networking sites. It can be observed that there are also many which are less obvious, such as monitoring and profiling the web pages an individual reviews and sharing this information with advertisers who target the individual with what they assume are interesting advertisements. In all such cases, there are more or less degrees of 'awareness' of the sharing of information, and the assumption is that the more aware a user is, the less invasive the sharing becomes as it is assumed to be voluntary. As the Information Commissioners Office highlighted at the Surveillance Society Conference in December 2007, individuals are increasingly leaving behind "electronic footprints which build up a picture of every aspect of their daily lives." Individuals may not realise that the data that is shared on sites, such as popular social networking or peer-to-peer networks, may be used for other purposes that the ones for which they originally provided the information.

The scope and methods of information sharing are therefore just one area of concern in personal information protection. They can in any event not be separated from the other principles relating to privacy: statements, reasonableness, security, access, use, and the ability to correct and delete personal information.

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments: The current Data Protection Act (European Data Protection Directive 95/46) effectively protects the lifecycle of data from its collection, processing to its

storage. However, the current legal framework does not address circumstances where data is lost or stolen. A legal gap therefore exists that needs to be closed particularly in light of the increase in incidents of data being lost or stolen occurring. The introduction of a data breach notification requirement under UK law would not only complement the current Data Protection legislation but also serve to enhance the security of personal information, shared, processed and accessed, in both the public and private sectors, throughout its complete lifecycle

Question 10.

Comments:

Question 11.

Comments: The effectiveness of the current Data Protection Act cannot be achieved solely by technological solutions. A co-ordinated approach to data security is required that recognises the need to educate and train people involved with personal data, have in place effective and appropriate policies and technological measures to ensure data when it is shared remains secure. It can be suggested that a key barrier to this approach currently is a lack of awareness and education to employees of the importance and value that is associated with individual's personal data. Consideration should be given to using training and skills organisations in the UK (for example Learn Direct) to provide a learning module or education programme on the importance of protecting personal data and the requirements of the Data Protection Act. Symantec has experience in developing online training packages for organisations around data security and would welcome the opportunity to discuss how an online training package could be developed and distributed.

Question 12.

Comments: As outlined above while the current Data Protection Act protects the data throughout its life, the legal framework does not protect information if it is lost or stolen. A recent survey conducted by Symantec in the UK found that 46% of those polled feel the legislation in place to keep individuals informed about the disclosure or loss of their personal data is inadequate.

This result not only suggests the current law needs to take into account citizens views on what happens to their data in the event of a data breach, but also and possibly more importantly the need to raise awareness on the measures and actions being taken by the public and private sector to ensure data is being protected. The proposed introduction of a data breach notification law under the review of the EU Telecoms Framework is seen as an important move in the right direction to increase levels of data security and also help raise awareness, and reassurance, amongst citizens across Europe of how their personal data is being secured and protected.

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments: It is understood that currently under existing legislation formalised data sharing gateways are in place between the public and private sector. The purpose of which are to enable information to be assessed against data stored on existing databases within a legally agreed framework. It is suggested that there may be public concerns over the use of data sharing gateways due to a lack of individual's rights over the access to information currently given. For example it is understood that while consumers consent to checks on their identity being conducted when applying for private sector services (such as financial services) when similar checks are conducted by public agencies these may be regarded as intrusive and leads to privacy fears. Public concern may derive from the fact that while financial organisations require an individual's consent before checks can occur, it is believed that no such consent is required in a data gateway investigation. Technological safeguards and legal protection can be implemented that can ensure the data provided through data sharing gateways is appropriate and relevant to the purpose for which the data is being sought. However, the transparency of the data sharing being conducted under data sharing gateways is suggested as a possible area for further discussion and consideration.

In conjunction with transparency reasonableness, as an overriding principle, is also an important tool in either a public or private sector organization's use of personal information. However, this does not lend itself to the development of an easy standard because reasonableness is sometimes a vague standard – and yet, hundreds of years of common law are based on the notion.

Question 19.

Comments: Privacy impact assessments can play an important role in ensuring appropriate data sharing. Not only does it require organisations to document and consider issues relating to privacy protection, and address mitigation of risks, it also creates accountability. It is suggested that the act of signing a privacy impact assessment as a manager in a public or private sector organisation, could suddenly help to crystallize the responsibility taken for data and encourage organisations to consider and ask the right questions, seek guidance, possibly legal advice and initiate action.

Section 5: Technology

Question 20.

Comments: In this era of pervasive technology personal information has become increasingly mobile. It is easier to gather and share personal information than it has ever been. Previously information gathered was limited to only as much as could be digested with pen and paper. This data enjoyed privacy through obscurity living in dusty file cabinets. However, today information can move at the speed of light and duplicated at literally no cost. That does not mean to say information cannot be protected effectively. Technological advances, such as the maturity of encryption technology, means there are now solutions commonly available which can assist in securing and protecting data. A particular aspect of encryptions maturity is the ability to centrally administer and manage encryption technology.

Another significant technological advance is data classification and data management procedures. The classification of data is the ability to designate appropriate security policies and access rights according to the level of risk to particular personal data. For example access rights given to staff can be monitored and audit trails produced, providing additional reassurance to citizens that the confidentiality of their data is being maintained. Access levels can also be used to dictate the information that can be shared outside an organization for example to another government department or private sector organization. These solutions can help to ensure data, which may contain personal information (for example such as an instant message or email) is automatically identified, encrypted or even blocked to prevent the personal information from being put at risk. Data classification also enables an organisation to develop standard policies, procedures and requirements for data management that can be regularly audited.

Question 21.

Comments: Given that technology evolves so quickly, the introduction of technological prescriptive legislation and regulations would not be appropriate or effective. For example in the area of encryption a standard could set a minimum level of encryption as 128 bit; currently considered to be the best practice level. There could however be technological changes that could make this too low a standard, such as discoveries of weakness in the encryption algorithm and/or a successful attempt to 'crack' the encryption technology. Also legislation and regulation can be slow to be promulgated in response to events and changes in technology. The law should not try to run behind or ahead of technology but rather set out a principles based approach based on assessment of risk. This approach can assist organisations to ensure appropriate policies, procedures and technologies but also allows for higher or lower safeguards to be introduced depending on the nature of the information concerned and the risk involved.

Question 22.

Comments: There is no doubt that privacy enhancing techniques are essential tools to

safeguarding privacy. The market offers a number of technological solutions and tools suitable for different environments and user-sophistication that can provide appropriate level of security and safeguards to protect personal sensitive information held by organisations. It can be suggested that 'best practices' statements from regulators could also be a useful tool in helping to educate developers and public and private sector organizations about their use. However, before the introduction of any best practice initiatives in this area, it will be vital that industry is fully consulted. In particular further discussion would be needed on how best practice statements could be developed that take into account the different data privacy issues that may differ between sectors and then how these statements could be promoted effectively to reach all sector and size of UK business.

In addition it is also suggested that the education aspect is also important to consider. In particular the perceived ongoing mentality in technology – one that now permeates the general public – that because the cost of data storage and backup is so low, all data can be kept forever. Privacy enhancing techniques aim to readdress this belief by leading organisations to consider questions such as the minimum amount of data needed for business purposes, how long is it needed for and the appropriate levels of access given to data.

While the information security industry will continue to develop easy to install and manage integrated security solutions, technology alone cannot be relied upon to protect information. Symantec believe a multi-layered approach to protect information assets is required that includes having appropriate technology in place, effective policies and procedures for data access and education and training on the importance of ensuring data security and privacy.

Section 6: International comparisons

Question 23.

Comments:

The Canadian Privacy Commissioners have a useful model, and experience, that on the whole bridges the approaches between the EU and the United States. While the powers of the various Privacy Commissioners vary, they have a very influential role and have been quite successful in taking a more mediation type approach involving educating organizations and the public rather than one based on sanctions.

For example, the Canadian Federal Privacy Commissioner has the power to audit organizations and the Ontario Privacy Commissioner has the power under the Personal Health Information Protection Act to fine institutions up to \$1 million (Canadian dollars) , and individuals (including health practitioners) up to \$250,000. While there is only one law in Canada that requires breach notification (Ontario's Personal Health Information Protection Act), the Alberta and British Columbia Privacy Commissioners have both considered that the obligation to notify arises out of the duty to safeguard personal information, which continues even after a breach. Even in Ontario, where there is

mandatory breach notification, the Privacy Commissioners' tend to view notification of their offices as essential and, in consultation with the organization, the Commissioners' determine whether a notice is required to affected individuals, and will not require notice (for example) where the breach is trivial or where there is the potential for more harm than is gained. Also in Canada there have been examples of joint investigations by the federal and provincial commissioners to permit sharing of resources and address situations of potential overlap in jurisdiction.

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments: There is clearly a difference in attitudes between the US and the EU in sharing of information as far as it relates to national security, as a result of the tragic events of September 11th, 2001. While it has often been said that there had been acceptance of intrusion into privacy from public authorities, there was no transference of this deference to the private sector. Americans are not dissimilar from Europeans in their concerns over private sector uses of personal information, and nowhere has this been more strongly shown than in the advent of mandatory privacy breach notification laws across various US states. Still, there is a difference in fundamental attitudes towards the management of personal information. The European Union, and other jurisdictions, have followed a legislative path with the view that privacy is a human right; whereas the US still typically regards personal information as belonging to the organization, with special obligations of stewardship in terms of its handling and management. Regardless of where each viewpoint starts, it is the case that good privacy practices are good privacy practices, everywhere, and the principles of privacy protection are the same.

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments: It is felt that it is important to consider data sharing along with other issues relating to privacy protection. There is sometimes a tendency to identify and single out 'a problem area', whether it is data sharing or another particular aspect of privacy such as behavioral analysis. While it is tempting to deal with each issue as it arises it is suggested that a more holistic approach is necessary and effective. This enables data sharing to be considered in light of other issues related to privacy protection. These may include existing privacy statements, reasonableness, use and disclosure, retention and security.

Furthermore, we believe it is essential that an internationalist stance is taken by privacy

regulators. Privacy protection is truly a global issue, and therefore requires adoption of international principles and standards in order to avoid creating and continuing a patchwork of inconsistent laws and regulations. Such an approach is essentially unworkable since information can and does flow between countries on a worldwide basis, and it should be irrelevant to the individual where their personal information is – it should be protected according to a consistent and fair standard. Finally, there is in reality not much that is different between the concerns of citizens of different nations, except experience and thus education of the risks. It is important to reach out and establish those international standards, even at times when it may appear that different countries appear to have very different perspectives on data protection and privacy.