

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:

- *Why we are interested in personal information and data sharing*

Demos is the think tank for 'Everyday Democracy'. The recent Demos pamphlet *The Everyday Democracy Index*¹ explored the factors that help determine how much influence and control people have over decisions, cultures and policies that affect them in their everyday lives. It develops the idea that, beyond parliaments and formal politics, we need to think about when and where people have the ability, capacity and desire to engage in the things that affect them.

Personal information has increasingly become one such area. It is relied upon by private and public sector alike to help them sort, judge and respond to people. As a result, it is of central importance in helping determine how these organisations respond to them. The decisions that get taken as a result - from credit decisions to the kind of welfare they receive - have serious implications for individuals and groups

¹ *The Everyday Democracy Index*, Paul Skidmore and Kirsten Bound, Demos 2008.

of people. Personal information helps to change the kind of services, relationships or treatment people experience.

Demos' interest in this area stems from a belief that giving people the opportunity to help shape collective norms, laws and policies on personal information is increasingly important. People need far greater influence over when and where they're information is used, and what it is used for. Currently, the balance of power is tipped too far in the favour of data holders. As a result, we argue that future policy making has to be centred around placing the individual at the heart of the flows of data concerning them.

Further, personal information use is increasingly important to the government's ability to achieve many of its policy objectives. A series recent trends have affected how government uses data. Technological changes have rendered personal information more vulnerable, cheap to store, and easy to copy and share. Personal information has as a result become associated with perceptions of government competency and capacity to tackle collective problems.

Combined, these make it vital that genuine openness, in the development of policy and practice and the communication of them, is placed at the heart of personal information policy in the public and private sector. Equally, it is important that government and private sector alike afford personal information use the gravity and seriousness it deserves.

- *Our work in this area*

The response draws on Demos' research into privacy and personal information. In Spring 2008, Demos will launch *UK Confidential*, a collection of essays on privacy by authors drawn from a range of disciplines examining the social value of privacy.

In December 2007 Demos launched the pamphlet *FYI: the new politics of personal information*², the result of a nine month research project into the implications of an increasing reliance on personal data in the public and private sectors. The research included expert interviews, case studies of organisational practice and focus groups

² *FYI: the new politics of personal information*, Peter Bradwell and Niamh Gallagher, Demos 2007

³ *The Future of Privacy*, Perri 6, Demos 1998.

⁴ *Divided by Information*, Perri 6 with Ben Jupp, Demos 2001

with members of the public discussing their attitudes to personal information use and privacy.

The pamphlet argues that because personal information policy and practice is too opaque, people are losing control over what people know and think about them.

Demos has previously extensively researched privacy, information use and the technological, political and social changes around it. *The Future of Privacy*³ set out the contemporary and future landscape of privacy, charting the technological, social and cultural influences shaping privacy. *Divided by Information*⁴ argued that the reliance on personal information means that increasingly, technology will mean a digital divide marked by exclusion *by* information, rather than *from* it.

All Demos pamphlets are available for free download, as pdf files, from the Demos website (www.demos.co.uk).

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

Question 2.

Comments: Driving the prevalence of personal information in both public and private sectors are the benefits, perceived or otherwise, of services or products tailored to individuals.

The past years have seen a drive towards a 'personalisation' of services in the public sector, supported by a government emphasis on efficiency and an increase in the availability of and access to new technologies. There is a longer-standing private sector approach to categorising customers according to tastes, behaviours and past choices, and shaping what they offer based on what individual customers want, need or aspire to.

The relationship between convenience and information use and sharing is close. To offer the personalised services we have become accustomed to organisations and governments have come to rely on millions of tiny parts of our identities, held together by increasingly sophisticated technology. There are a plethora of real benefits to this.

This helps explain why it is impossible to separate the benefits of an open information society with the challenges associated with giving away so much information about ourselves. The key is to ensure that in navigating that tension, people are given the ability to help influence information policy, ensuring that the way personal information is used is driven by those interests as much as commercial or political interests further from their grasp.

In the context of individuals' interactions with the private sector, convenience is perhaps the most obvious benefit of information use. The ease with which one can find, purchase, and be offered products and services has seen, for example, an incredible growth in e-retail (the value of e-retail stood at £4 billion in July 2007⁵).

Further, the appeal of peer-to-peer information sharing has seen a huge take-up of social networking sites, and other online tools. These allow people to connect and collaborate in new ways. An important benefit of openness with personal information is that it allows more people, potentially, to play a part in what more institutional surveillance has traditionally been about - sorting, judging and responding to the people and ideas around them.

An example of this might be eBay's peer review system, in which users rate each other according to the successes or failures of previous transactions.

In the context of the use of information by government, individuals can potentially experience better service from providers where they hold details about an individual that informs the kind of service offered. Medical research can be greatly aided by the wealth of information available from people's experiences of illness and disease.

Question 3.

Comments: By sharing personal information we surrender control in the longer term by leaving ourselves open to judgement by different groups in different ways. The drive to personalise or tailor services, which is shaped by those judgements, can lead to differences between what people experience and have access to. This can mean a narrowing of experience, can lead to social exclusion, and has significant implications for how we live together as a society.

⁵ 'e-Retail hits 80% hypergrowth – £4bn web sales in July', IMRG, Aug 2007, see

These dangers will emerge if debate now is not open, meaningful and ongoing. Without that, there is a greater risk that people lose control over their information.

Individual

For the individual, this can mean a lack of control over decisions that affect them. The danger is of giving others – government or business – the tools with which they can take important decisions out of people's hands. Further, the traditional battle to ensure that undue and unwanted surveillance and intrusion from others remains. There is a risk that these less tangible concerns become outweighed by perceived more bureaucratic benefits.

There is also a risk that a lax attitude to personal information can mean that it is not afforded the care it deserves. Information can be personal not just because it is about an individual, but because it is of deep significance to them. For example, in medical research, there is a risk that people's sensitive details of illness and course through the disease is open to scrutiny by more people than they might be comfortable with. This is not a case of stopping the sharing of data, but of ensuring it is treated with appropriate gravity and care.

Society

The consequences of refining services lie in a potential reinforcing of distinctions between people and a narrowing of experience. This makes it more likely that our cultural 'diet' will be more acutely defined, and reduce exposure to other ideas, people or sources of information. On the one hand this is a good thing – it means people can potentially stitch together their own cultural experiences. Through the things they eat, see, read, consume and share people have the tools to negotiate a sense of self. But on the other hand, it poses a problem for a political system that is predicated on a healthy public realm.

Information held about us can influence our experiences, contribute to social exclusion and, through a dearth of debate, damage the public realm, but that is not all. There is a danger that we forget the distinction between the process and content of categorising. Though the process is automated, the categories into which people are sorted are devised by other people, and reflect the social distinctions of our

⁶ *Seen and Heard: Reclaiming the public realm with children and young people*, Joost Beunderman, Celia Hannon and Peter Bradwell, Demos 2007

society.

Once ingrained, perceptions of difference are difficult to shift. That includes both how institutions and businesses see people, and how people see themselves. The danger is that the fragmenting of experience that results from exclusion by information can be reinforced by the technology and architecture built around divisions and rights of access.

Parallels exist between this process and what is happening to public space. The Demos pamphlet *Seen and Heard*⁶, for example, found that the economic rationale that plays a central role in how many places are organised has contributed to the exclusion of young people from public space. It is often economics that determines and justifies how many different spheres of life are sorted and judged, which impacts on the kind of behaviour and activity that is encouraged or punished. Information surveillance is often deployed as the means to enact that 'control' in regulating the rules and success and norms of behaviour.

It is important that these less tangible, longer-term challenges associated with segmentation are considered and policy built around an appreciation and understanding of, and open public debate around them.

Question 4.

Comments: The most important factors in how personal information use is the sharing of different types of data, in different contexts, in ways not envisaged or understood at the time the data was given away or acquired. This can happen through the combining or cross-referencing of data sets. This is an increasingly important challenge given the lowering costs of storing large amounts of data.

For example, the knowledge of whether someone is being watched, and by whom, helps to determine how they behave and the sort of information they reveal. So, clarity over what kinds of judgement are going to be made, and by whom, informs decisions over willingness to give away details.

An important factor in this is the merging of public and private sector roles. This developed through the contracting out of public service delivery to the private sector in the 1980s, and has progressively blurred the distinction between the two as their functions intertwine. This has served to exacerbate the questions of power, responsibility and coercion in both. This merging coincides with an increase in demand for good quality, comprehensive data, and competition among data

suppliers, making connectable information about every aspect of an individual's life easier to come by than ever before.

Personal information has become, as a result, less easy to segment in terms of what is relevant for public or private sector purposes. One of the clearest examples of this trend playing out is through credit agencies, which provide the information that forms the basis of risk judgements by others – such as banks and loan companies. Having traditionally been tasked with checking customer credit ratings for banks, mortgage providers and estate agents, they are now under pressure, from government and business clients, to increase the types of data they hold – going beyond credit towards lifestyle choices and behaviour – in order to give a more complete picture of the risk, or level of 'trustworthiness', associated with an individual.

The result is that credit agencies become involved in decisions that are not about credit. The availability of this kind of information risks decisions being made about people on unfair grounds – in the future, armed with comprehensive data about clients, firms may be able to choose customers rather than the other way around. The life insurance market, for example, which traditionally pooled the risk of high- and low-risk clients, might choose to exclude people with poor access to health care or particular lifestyles, based on the level of risk they pose.

Question 5.

Comments:

Question 6.

Comments:

One risk in the private sector is from the merging between or takeovers of large companies, particularly in the context of large web- or technology-centred firms, which draws together data sets. One example might be Google's acquisition of online advertising firm DoubleClick. Without presuming any specifics of the case itself, it is an *example* of the need to ensure that in such cases the integrity of personal information remains. That holds true for the security of the data, but also the new contexts into which information will be applied and used, for example.

Question 7.

Comments:

One area of personal information sharing given too little attention is the sharing of data between data holders and the data subject - or, between organisations and the public. Currently the relationship exists in a cold, legal sense - the public have a right to access the data held about them. This should remain, and indeed be extended, as detailed below.

However, there is a significant opportunity to take advantage of people's willingness to engage in a world of open information use and, securely, develop services based on sharing people's data with them. For example, in London, Transport for London could offer Oyster users, for a small charge, in-depth reports on their travel habits, perhaps in the form of visual maps. This would have to be governed by strict rules on rights of access, for example. It would build on people's interest in social uses of personal information, that help them map and understand the world around them and their interactions with it.

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments: The DPA plays an important role not only in setting a rigorous framework for the protection of people's information, but, in its success at doing so, plays an important role in influencing public trust in personal information use. A key principle for the Data Protection Act and its development should be to place the individual at the centre of the information flows concerning them. In that context, there are three main changes we would advocate in the development of the DPA.

1. Powers to enforce the Act

Because of the dual role highlighted above, it is vital that the authority with responsibility for overseeing the DPA's implementation must have demonstrably greater powers to enforce it. This extends to the public and private sector. This should involve criminalising negligent personal information use; and enhancing resources to improve compliance, for example.

2. Accessibility and language

The DPA is an Act that covers an area of policy, law and practice that has an increasing influence over people's lives. Further, it is not just the actions of lawyers, policy makers and businesses handling personal information that influence how personal information is used; how prevalent it is; and where it is given away. People themselves do and should play a big role in determining the personal information landscape through their everyday interactions. They need to be able to understand the regulations, rights and responsibilities afforded to them by the Act. These were highlighted through our qualitative research as particular important factors in

people's attitudes to personal information use and their privacy.

So both in its content and presentation it should encourage openness and accessibility of policy. It should be another tool to encourage engagement with and accessibility of the laws and norms around personal information use. Firstly, that means requiring organisations' and institutions' data protection policies to be written in clear, non-legalistic language. For example, it could require a common-sense test for privacy policies. Secondly, the Act itself should be accessible, meaning that the rights and responsibilities it implies are clearly laid out.

3. Rights of access

The rights of access individuals have to information held about them in the private sector should be extended, including the right to know what groups people have been 'segmented' into, and allow greater ability for individuals to challenge and change existing information about themselves that they believe to be invalid, incorrect or unfair.

Question 10.

Comments: The second principle is both incredibly important, but equally challenging given the difficulty of specifying the purpose with the appropriate definition. In other words, it can be difficult to specify exactly what purpose information will be used for in a way that is either not too constraining on future use, or not so vague as to be meaningless.

As suggested in the response to question 4 above, this is an area of increasing concern. Given the prevalence of, and ease of access to such a range of data its connectability, future relevance and future significance become more live and pressing concerns.

The second principle is so valuable because it sets the context in which information is used. That information becomes meaningful through that use. If people are to be more empowered to influence the way their information is used, then there needs to be a focus on the purposes it is used for, and the possibility of influencing and challenging that use.

Currently organisations are not clear enough in the purposes they are putting data to now, and when and how that might change.

In the public sector, for example, the exact purpose of the identity card scheme has veered across a number of differing explanations, each with differing implications for people's willingness to see the scheme progress. That particular debate needs to restart, ground up, driven by a refreshed openness of policy and guided by the interests and needs of the public.

In the private sector, firms can be too opaque in their use of personal information. One example is how some businesses use data for marketing purposes. For example, it is often unclear exactly how technologies around email and website use tracking work, and how the information given away as a result shapes the resulting service.

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments:

- *Published personal information compliance results.*

This could, for example, mean more pro-active openness from organisations with support from the Information Commissioners Office. The Freedom Of Information Act has seen health and safety inspections for restaurants published online, creating a forum for the public to see the standards of restaurants and cafes. In turn, this becomes a mark of pride and pull factor for more proactive publishing and standards from those outlets. There are similar opportunities in the area of personal information. Given the interest from the public in data policy, there is an incentive for

business to become more open and demonstrably compliant with the DPA and good practice principles.

Businesses could publish the results of Privacy Impact Assessments, for example. There is also an opportunity to proactively seek compliance and good practice tests, similar to health and safety schemes, which businesses could then publish publicly. Funding for this could, for example, come from a combination of increased public funding to the ICO and the charging of a reasonable fee by the ICO for the inspection.

- *Common-sense tested explanation of flow of personal data within and from organisations.*

Businesses and departments should be compelled to produce simple, easily understandable explanations of their policy and practice relating to the use and sharing of personal data. To do this a 'common-sense' test, as described elsewhere in the answer to question 9, could be used. This could come in the form of visual maps and easy-read policy explanations, covering both the practice of personal information use and the rights and responsibilities of the organisations involved.

- *Cross-sector debate led by the Information Commissioners Office*

As a bridge between people, policy-makers and technologists, a body such as the ICO should be given the remit and resources to lead open discussions and debate to help build more secure, effective and appropriate technology for personal information.

Question 19.

Comments: Data and facts retain a significance well beyond the convenient transactions they may have been generated by. Democratic policy - transparent, accountable, open and something people have a stake in influencing and shaping - on personal information, means maintaining the spirit of collaborative openness that information technologies promise. To achieve that, we need collective rules about when and where individuals have the right to control, or influence, the use of the information that increasingly determines their worth.

To help achieve this, for example, each department and organisation should hold an open debate about how and why it uses personal information, and allow the public to influence the way that personal information shapes the service or relationship.

Section 5: Technology

Question 20.

Comments: Firstly, online tools have made it easier to collect information about people. That can either happen in contexts where people know it is happening - filling out forms, for example - or in contexts where this is less the case - email tracking tools, for example.

Secondly, with the consequent masses of data, and the declining cost of storage, it is clear that information is more vulnerable to attack. Many more people have the tools to acquire data fraudulently and use it for financial or other criminal gain.

Thirdly, perhaps one of the most significant trends that technology has helped exacerbate relates again to the tailoring of services to individuals. The debate about 'network neutrality', for example, serves as a good example of how the 'flat' design of the internet and open information tools might be changing. The debate concerns the concentration of access and traffic in a small number of telecommunications companies. It focuses on the implications of distinguishing between internet users based on their ability to pay, systematically prioritising, for example, the traffic of a City finance firm over a grandma from East Ham.

The long-term consequences of this damage the principle of the 'flatness' of access, which is borne of the blindness of intent the internet architecture was built around. Instead, it builds in decisions about what kinds of activity and people the technology should serve and promote. This is indicative of the internet's direction of travel in terms of content, too – away from a series of connected documents, towards bits of data connected through the meaning people give to them.

Tools like search engines are seen as empowering – giving people

access to new sources of information. But just as in the debate around net neutrality, technology is starting to embody a particular kind of limit to access by shaping what is on offer around decisions about who you are. This is about inserting context and meaning back into words and associations of words, with the inevitable consequence that they become more relevant or appropriate for some people than others.

So technology can exacerbate the trend towards a tailored service or product. Personal information plays an important role in determining what that service looks like. But it can also play an equally vital role in ensuring people can influence and shape what it looks like and who finds out what, and what they decide as a result -

through open, user-centric 'Digital Identity Management' (DIM) architecture.

We do not expect to exert full control over what is said, known or thought about us. Bits of information are needed about us by others, usually governed by principles or rules about when and where it is appropriate for people to have access to that information. So, for example, if we want to buy a house, then the bank lending us the money to do so might run a credit check – the information fed to them is the basis on which they can make a judgement about the kind of people we are. Less instrumentally, people need to share and learn about others; to share thoughts and feelings to build a sense of understanding over the world around us. Usually, there are means of redress if a person believes another's opinion is incorrect or damaging in some way.

'Digital identities' – either the ones we actively help produce or the identities held in electronic form by institutions – are increasingly as intimately a part of these processes as people's offline selves. Personal information is the raw material for this, and DIM technologies can help us answer a simple question: how do we think we should prioritise claims over how personal information is managed?

It is important that identity systems are built with the person at the centre of their information flows, and user-centric models should play a crucial role.

Question 21.

Comments:

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:
