Share and share alike - attitudes towards data sharing in the UK public sector

Marion Oswald, Solicitor and Head of the Centre for Information Rights, University of Winchester, and former Central Government Legal Adviser, discusses personal data and trust, in the context of research into attitudes to sharing personal data with the UK public sector

About the research

'Altitudes to Sharing Personal Data with he Public Sector' — copy available at www.pdpjournals.com/docs/88155

The Oxford Dictionary defines 'to share' as 'to apportion (something) among others.' In everyday language, we often use the word to mean giving something to someone (perhaps temporarily) or letting someone 'have a go.'

We tell our children to share — share your toy with little Jonny, we insist righteously, although (secretly) we do not trust little Jonny not to break it. As adults, we tend not to apply the same standards to ourselves. If we share, we want safeguards; when we share our money with a bank, we want the government to guarantee our savings; if we share our ideas, we want to know that someone will not copy them; if we share our property, we want to know that someone takes responsibility for any damage.

And what about sharing our personal data — what assurances do we want? The potential for damage is so much more difficult to quantify compared to, say, the sharing of physical property. Philosopher, computer scientist and political writer, Kieron O'Hara has said that "there are many tangible benefits to be gained by allowing intrusions into one's life, but there is also the intangible worry. We simply find it hard, as humans, to balance the tangible benefits and the intangible costs."

Our decision may come down to first, what benefits we believe we will gain by sharing our data, and secondly, whether we trust the organisation that acquires our data.

Sharing — the challenge for the public sector

Collection of personal data, and transfer of such data from one public sector body to another, or within a public sector body, can be of fundamental importance to the successful delivery of public services, the identification of risk and the discharge of government responsibilities.

Take one example of data sharing between public bodies: safeguarding. The Serious Case Reviews into the death of Keanu Williams and Daniel Pelka criticised the robustness of data sharing between public bodies. The Keanu Williams Serious Case Review said that it was 'clear that if everyone had known what others knew there may have been a very different outcome.' The Daniel Pelka Serious Case Review commented that 'instances of concern tended to be viewed in isolation with a lack of attention to the patterns developing.'

Compared to sharing personal data with, say, an online shopping site or social media service where the benefits to the individual may be tangible but the costs less so, the reverse may be true for sharing personal data with the public sector. The benefits for the individual may not be immediate or obvious, but the risks — or perceived risks based on reported data breaches, fear of a 'surveillance' society, concerns that anonymised data could be re-identified, and what O'Neill has described as 'a culture of suspicion' — are much more apparent.

My recent research into attitudes to sharing personal data with the public sector in the UK explored participant's opinions on providing locational and medical data to local councils, central government and the National Health Service, and how personal data are used and shared by those organisations.

Lessons to be learned from the research

Trust in the NHS is high: The research indicated that the NHS was the most trusted sector. 79% of participants were very or fairly comfortable with the NHS collecting, storing and using detailed medical history, compared with only 8% for local councils and 11% for central government.

Websites/search engines are perceived to be more trustworthy than local or central government organisations: Comparison with research conducted by law firm Osborne Clarke suggests that people are more comfortable providing websites and search engines with their medical information than providing some information to the local or central government.

This could be due to the so-called 'culture of suspicion' that surrounds central government. Also, when people provide websites or search engines with medical data, it is most likely that this is to investigate and locate information about an ailment, thus providing the individual

(Continued on page 16)

(Continued from page 15)

with an immediate benefit perhaps not so apparent when providing data to central or local government.

Sharing is a scary word: Comfort levels with all organisations dropped when participants were asked about organisations sharing personal data: 22% were comfortable with the NHS sharing detailed medical history, dropping to 2% in respect of local councils sharing detailed medical history and 6% in respect of central government sharing location information.

Anonymisation makes (a bit) of difference: Results demonstrated higher levels of comfort with anonymised data being used or shared; for instance, the comfort level with central government sharing location data rose to 38%.

One participant commented that "most data to assist public services can be anonymised, but I fear is not." Another expressed the view that "if my personal data were anonymised, I would answer 'very comfortable' [to different uses of data] as I believe that public sector organisations should only base their changes or improvements on factual data rather than 'finger in the air' responses."

Anonymisation made no significant difference to people's comfort levels regarding the NHS collecting, storing and using personal data (74% for personal data, 75% for anonymised data). This may indicate that people have a high appreciation of the need for the NHS to use personal data, although it begs the question as to why a quarter of people surveyed were not comfortable with the NHS using personal data.

Trust is fragile: Only 8% of survey participants said that they would be willing to share their data following a security breach, one participant commenting that "I am more concerned about data security (breaches/loss of data by central and local government) than I am about deliberate sharing."

The Information Commissioner's Office has reported that 137 data breach incidents occurred in the health sector in the second quarter of 2013, the highest of any sector. Trust lost as a result of such incidents may be hard to salvage, though as the ICO itself points out, NHS organisations are required to self-report potential data breaches.

Are these figures giving a misleading impression of the risks in the health sector compared to other sectors where self-reporting is not mandated?

Altruism versus personal interest: The individuals surveyed showed a high level of willingness to provide their information to improve public services, but were more reluctant to do so when money was mentioned, even when the money was to benefit public services.

Participants were mostly altruistic about the use of their data to prevent or investigate crime, but were more nervous when this could mean monitoring of their own behaviour.

Although 85% of participants said that they were very or fairly comfortable with their personal data being used to improve delivery of public services, only 32% were comfortable with data being shared with other public sector organisations, and less than 10% were comfortable with data being shared with commercial organisations.

On the face of it, the results show that people are reasonably comfortable with personal data being used for altruistic or public purposes, but using the term 'sharing' appears to reduce comfort levels significantly and may indicate a lack of understanding of the underlying reasons for data sharing.

As one participant put it, "I feel there is a lot of sharing which occurs within the public sector which is not made clear to the public".

Final thoughts

It is unfortunate that the word 'sharing' has become shorthand for the disclosure of data by one party and the acquisition by another. While often simultaneous, acquisition and disclosure are separate activities in law, and data may not flow both ways. It may be that a lack of clarity around the reasons for disclosure and corresponding reasons for obtaining data, in favour of the catch-all term 'sharing', contribute to a lack of trust in the public sector's motives for disclosure and acquisition of personal data.

So I would like to pose a number of challenges for 2014: that we closely examine our own attitudes to the sharing of our personal data. How do we assess risk or decide who to trust - based on sober assessment of evidence and relevant law, or on gut-feeling? Are we motivated by personal benefit or by consideration of wider societal benefits?

For those in the public sector involved in making data acquisition and disclosure decisions: how can transparency around the reasons for data acquisition and disclosure be improved in order to address the 'culture of suspicion'? Can confidence in the anonymisation of personal data be improved? Is there an issue of trust between public sector agencies resulting in a 'the data that I hold is too secret/sensitive/important to be transferred to you' attitude?

I'd like to close with something I read recently about the late Nelson Mandela. Asked whether Mr Mandela had a weakness, South African anti-apartheid activist and member of the African National Congress, Walter Sisulu, thought for a moment and said: "He has a tendency to trust people too much…". Upon reflection, Sisulu added: "But perhaps that is not such a weakness after all."

Marion Oswald
University of Winchester
marion.oswald@winchester.ac.uk