

Legal Regulation & Education: Doing the Right Thing?

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

SHARE AND SHARE ALIKE? TRUST, ANONYMISATION AND DATA SHARING

In the context of ongoing issues surrounding the sharing of personal data with, and between, public sector bodies, this paper will review the results of an exploratory research project into attitudes to sharing personal data with the public sector. It will investigate how trust correlates with attitudes towards sharing personal data with various organisations and institutions, and review how the benefits and costs of sharing are balanced. It will compare attitudes to sharing with the public sector with other surveys that have assessed attitudes to sharing with the private sector, and consider whether anonymisation of personal data makes any significant difference to comfort levels. Finally the paper will challenge widely held attitudes to the collection and use of personal data by the public sector – is society as a whole doing the right thing or are our attitudes and actions infected by a ‘culture of suspicion’ and a misunderstanding of the term ‘sharing’?

Research Method

The research, which was carried out between May and August 2013, was funded by a research grant from BILETA and carried out in collaboration with Hampshire Hospitals NHS Foundation Trust. A sample of 131 adults took part in the study. Participants were recruited via self-selected sampling, with questionnaires being available in a NHS hospital reception and online. A 102 item questionnaire was compiled, both in paper and electronic formats. Questions focused on participant’s opinions on: providing location and medical information to local councils, the central government and the NHS; how personal data is used by public organisations; anonymised data; privacy terms and conditions, and demographic information.

Results

The paper will compare levels of trust in the NHS, Central and local government and further compare with surveys relating to the sharing of medical information with websites and search engines. Results indicated that comfort levels dropped significantly when the term ‘sharing’ was used, with participants demonstrating particular concern around recent high-profile data breaches. On the face of it, results showed that people were reasonably comfortable with personal data being used for altruistic purposes, but using the term ‘sharing’ appeared to reduce comfort levels significantly.

Argument

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.

But 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.

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 a the catch-all term ‘sharing’ contributes to a lack of trust in the public sector’s motives for disclosure and acquisition of personal data.

The paper ends by posing a number of challenges. 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? And 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?