Private lives in a database world

Richard Thomas CBE

Annual Lecture for the IT Faculty of the Institute of Chartered Accountants in England and Wales

6th December 2010

Richard Thomas gave the IT Faculty's annual lecture in December 2010. Richard was the UK Information Commissioner from 2002 – 2009 and now advises the Centre for Information Policy Leadership, the think tank associated with law firm Hunton & Williams. His lecture focused on the challenges to data protection caused by the pace of change with new technology, and the need for a modernised and globalised regulatory environment for personal information.

Technological and political change
Richard first coined the phrase 'Sleepwalking into a surveillance society?' in 2004. Since then, technology has continued to evolve and increase the risks surrounding personal data. The rapid growth in powerful mobile devices, cheaper and greater data storage capacity, more effective analytical and aggregation tools, smart and ubiquitous computing with chips embedded in everyday items – the opportunities to gather and analyse information about us, our locations, our activities and our preferences are seemingly endless.

These changes have not gone unchallenged, with growing media and public concern about privacy. Businesses such as Google and Facebook are under constant scrutiny and pressure with their privacy practices. There has also been a change in political tone, with a roll back of many privacy-sensitive public sector databases such as identity cards.

However, the pressures remain. Fears around terrorism and security provide a stark counterbalance to privacy concerns and encourage the retention of data. Furthermore, businesses continue to innovate and provide new, and often free, services based around the use and exploitation of personal data. As a result, the protection of personal information has become increasingly complex and contentious.

Building a good regulatory environment
The EU has a well established data protection regulatory regime. However, while the principles of data protection are very broadly accepted, the real challenge is to translate those into workable practice. Indeed, the 'holy grail' of data protection regulation is to find practices that effectively protect individuals without being too burdensome on businesses. So, what makes good regulation in this area, and what should be avoided?

Richard firstly argued that regulation should be based on the risks presented by personal data, with greater clarity about the harms that can arise. These could include harms to individuals – economic, social and to their dignity – harms to organisations and harms to wider society, such as damaging relationships and reducing trust. However, these harms need to be balanced against the substantial benefits which can be gained from using and sharing personal information. As a result, regulation should be increasingly focused on how personal information is used, and the outcomes to avoid, rather than its simple collection and processing.

In contrast, regulation that is unduly focused on prescriptive processes is likely to be burdensome to business and unlikely to be effective. Richard was particularly critical of the EU notification requirements in this regard, citing them as outdated, pointless and excessively bureaucratic.

Broader challenges to good regulation

The broader business environment presents particular challenges to good regulation of personal information. The international dimension, for example, creates particular problems, with regulation based around national boundaries. The EU also restricts the flow of personal data to other countries without adequate protections in place. As many businesses have substantial global elements, this can make compliance massively complex.

Social attitudes and norms are also changing very quickly. For example, being on a social networking site a few years ago may have been seen as a minority activity. Today, with Facebook the equivalent of the world's 3rd largest country, non-membership of such sites is more likely to be out of step with the majority. Regulators should not judge the rights or wrongs of these evolving social norms, though. Rather, they need to reflect and 'gently lead' some of these changes, where appropriate.

Organisational accountability

At the centre of Richard's approach is the notion of accountability. While accountability is a well established principle in other spheres, he argued that - although it features in the OECD Guidelines of 1980, there is scope for much greater emphasis on the concept in the field of data protection. He outlined 2 main elements to the vision of accountability:

- Businesses should be able and encouraged to ***tailor*** a structured approach to complying with Data Protection Principles within their own business model. He argued strongly that 'one size does not fit all' and that, while there need to be general principles and minimum standards, each business should develop an approach that is based on the specific risks arising from the ways it handles personal information.
- Businesses should be ready to ***demonstrate*** adherence to their own rules and approach and be held accountable for doing so. There are many elements to this, such as transparency and 3rd party or self validation. Richard also argued that there should also be more meaningful sanctions where businesses fail to live up to their standards or where they provide misinformation on their practices.

By making businesses more accountable in this way, data protection can move from being a tick box, compliance exercise to something more meaningful in the business, with executive support and priority.