Editorial

Bridget Treacy introduces Volume 11, Issue 4, of Privacy & Data Protection by considering whether consumers are losing interest in data protection

In November 2010, the first fines imposed by the Information Commissioner's Office ('ICO') for breaches of the Data Protection Act 1998, received widespread publicity. Just three months later, the ICO has imposed two further fines for data breaches (£80,000 for Ealing Council and £70,000 for Hounslow Council, following the loss of unencrypted laptops), yet these breaches (and monetary penalties) have barely registered in the public consciousness. Clearly, reaction to data breaches is not the true measure of public interest in data protection, but wider comment might have been expected. International Data Protection Day also came and went (on 28th January) with limited public acknowledgement in the UK. Are consumers losing interest in data protection?

Some insights into consumers' views may be gleaned from the ICO's annual awareness research (concluded in November 2010 but released by the ICO on Data Protection Day). The report indicates that this year fewer individuals (60% compared with 67% in 2009) feel that they have lost control over how their personal information is collected and processed, yet only 56% considered that organisations handle personal information in a fair and proper way, and a mere 37% consider that online companies collect and keep personal details in a secure way. These results are broadly consistent with previous years' results. Yet, despite these concerns being expressed year after year, people reveal ever more about themselves online.

Organisations are responding to this by deploying data analytics to observe and predict ever more about individuals. There appears to be a growing awareness of data protection sensitivities when collecting and using data in newer contexts. One such example is the UK Government's recent launch of its crime mapping service, which seeks to provide information about crime statistics to local communities. Given the likelihood that an individual may be identified where a particular crime can be linked to a particular address, the police crime maps show aggregated numbers of incidents mapped to a nearby area. The maps therefore yield little more than a general overview of crime levels in a given location but, in response to the initiative, the ICO has published guidance on the privacy implications of crime mapping activities. In this guidance, the ICO acknowledges the societal benefits of the crime mapping tool and welcomes the "drive to improve accountability through greater transparency".

In this context, the ICO's focus on improving accountability through transparency potentially has much wider application, particularly for organisations that use analytics. A particular focus of the ICO's guidance is to encourage organisations to undertake the mapping activities at a sufficiently high level of generality so as to reduce the likelihood that an individual will be identified. The ICO urges organisations to consider the granularity of their activities, the regularity of data uploads, the sensitivity of the crime, the information recorded on the map, and the availability of other sources of information. In particular, the ICO urges organisations to focus on the likely impact of their activities on an individual, and to make use of Privacy Impact Assessments as part of this analysis. Significantly, the ICO also encourages organisations to be aware of other sources of publicly available information that may be combined with the crime map and lead to the identification of an individual.

Although this guidance has been produced in the specific context of crime-mapping it has much wider application in the context of data analytics. Organisations of all sizes increasingly seek to use data to inform them about their customers and to help predict consumer behaviour. Organisations of all kinds seek to use data for secondary purposes, raising issues as to the scope of data processing permitted under the initial purpose, and requiring close analysis of the scope of any secondary purpose for which the organisation may wish to use the data.

The ICO's focus on improving accountability through greater transparency should be a key focus of the current debate on reform of the Data Protection Directive. Transparency has long been a cornerstone of data protection regulation, but accountability has received less focus. Linking transparency and accountability does not dilute or remove the need for legal compliance, but focuses attention on an individual organisation's conduct and creates an expectation that its data processing activities will be deliberate (rather than accidental) and that the organisation will be in control of and willing to take responsibility for those activities.

In the arena of data analytics, consumers frequently complain of a lack of trust (a theme which appears consistently in the ICO's annual survey). Focusing on how organisations demonstrate their compliance with the Data Protection Act, whether through a Privacy Impact Assessment, or by other means, in conjunction with an increased focus on transparency, may reassure consumers. Organisations benefit when consumers trust them, and should seek to build this trust.

Bridget Treacy
Hunton & Williams
btreacy@hunton.com