Editorial

Bridget Treacy considers the challenges ahead for Volume 10, Issue 3 of Privacy & Data Protection

As the privacy community turns to anticipate the future shape of privacy and data protection, there is much from last year that will influence not only the year ahead but also the next decade. Many of the issues are not new; the challenge for privacy professionals and their advisers is to adopt a pragmatic yet measured approach to overcoming these. With the Data Protection Directive and its implementation under active review and discussion and the prospect of change a real possibility, now is the time for privacy professionals to think carefully about their privacy priorities. A number of key themes should remain at the forefront of privacy officers' minds.

The Information Commissioner has signalled a tougher approach to enforcement. His long awaited powers to impose monetary penalties for serious breaches of the Data Protection Act will take effect in April, and the upper limit for a penalty will be £500,000. With a Commissioner who readily admits that he intends to make use of the power to impose penalties, perhaps imposing as many as twenty penalties in the first year, attention will inevitably focus on the unfortunate early recipients of these penalties. For privacy officers, the arrival of fines for serious data protection breaches is an opportunity to raise the profile of privacy issues internally.

Security breaches will continue to generate headline news. European lawmakers will continue to seek a general security breach notification requirement. Also, as has happened in Germany and has been discussed in France, individual States may take unilateral steps to establish their own notification requirements in direct response to political pressure and local breaches. It is hoped that lessons from the US are learnt and that our European lawmakers seek to develop a consistent approach to notification, which is subject to a harm threshold. At a practical level, and building on US experience of data breaches, a challenge for privacy officers is to ensure that their objectives and resources are closely aligned with those of data security teams.

Concerns about online privacy and behavioural targeting are now widely aired and are the focus of the consultation of the Commissioner's Office into online privacy issues. The explosion in the use of social networking sites, particularly in the last twelve months, has brought these challenges to the fore elsewhere too. Online privacy is a key focus area for the US Federal Trade Commission for 2010. In the UK, we can expect greater scrutiny of privacy notices and increased consumer demand for greater transparency and choice in relation to data processing activities. In the US, leading privacy experts are questioning whether the 'notice and consent' model remains valid in an online world. Privacy officers would do well to revisit their online data collection and processing activities and to ensure that these are consistent with their customers' expectations.

Cloud computing, widely discussed in privacy circles, has become the conference programme topic de jour. There is much scare mongering surrounding cloud computing. The movement of data to the cloud is inevitable — the model represents a fundamental shift towards utility computing — and the challenge for privacy officers is to mitigate and manage the associated risks as mainstream risks for the business.

International data transfers will continue to challenge businesses and we will continue to see a range of approaches to satisfying the EU's requirements for international data transfers. We await the imminent release by the European Commission of a new set of controller to processor model clauses that are expected to assist outsourcing transactions in particular. This may also be a bumper year for Binding Corporate Rules approvals, with regulators becoming overwhelmed by applications as organisations gain confidence in the process. Further, the Article 29 Working Party's recent endorsement of the adequacy applications made by Israel and Andorra may encourage other countries to consider this route for data transfers.

On a grander scale, the European Commission has raised expectations for reform of the Data Protection Directive by inviting comments on its future. Submissions closed on 31st December 2009 and are being published on the Europa website (www.europa.eu). This is the start of a lengthy process, but there will be many opportunities to debate the future of privacy, and privacy officers must stay informed and contribute to this dialogue. We will also start to see wider discussion of the likely impact of the Lisbon Treaty on data protection issues, particularly in the area of policing and law enforcement.

So, what does the crystal ball hold for privacy professionals? Many challenges and continued job security. In our networked world, data is a key asset and data protection and privacy issues are mainstream issues. There is much work to be done in 2010 and beyond.

Bridget Treacy
Partner, Hunton & Williams
btreacy@hunton.com