Regulators push for privacy audits

By Alan Pedersen

PRIVACY COMMISSIONERS ARE KEEN to encourage more independent data protection audits. But can they persuade the corporate sector that it is in their best interests?

The use of auditing as a tool for privacy compliance is gathering momentum. Its exposure to the business community has been highlighted through a number of recent enforcement cases. Only recently, high profile US corporations – including Microsoft and DoubleClick – hit headlines in the mainstream press after agreeing to implement independent privacy audits in their settlements with federal and state regulators. Although the number of organisations carrying out audits is rising, growth is still relatively slow. It seems it may be some time before privacy auditing becomes common practice.

Approaches to auditing

There is no standard approach or one-size-fits-all methodology to privacy auditing. It can be carried out by internal compliance departments, national data protection authorities, or by a range of privacy, IT and legal consultancy firms – all with different approaches. How complex and exhaustive a privacy audit will be varies between businesses. Some organisations audit their practices against their privacy policies – as in the cases of Microsoft and DoubleClick – while others will conduct a more extensive audit to bring them firmly in line with specific privacy laws.

Regulatory authorities favour the more extensive audits, regarded as one of the most effective ways for an organisation to achieve compliance with their legal obligations. Auditing against privacy policies is no guarantee that legal compliance is being met, as these policies only represent one facet of an organisation's privacy obligations. There may be areas away from the commercial side of the business – how workers' privacy is protected, for example – that are being neglected.

In an effort to encourage the more extensive audits, some countries – such as the UK and the Netherlands – have drawn up precise guidelines to help businesses carry out full data protection audits (see notes for details).

Forced privacy audits

During PL&B's September International Auditing Roundtable, delegates explained that the legal approach to auditing is not always entirely clear. Many data laws do not explicitly grant privacy regulators powers to audit organisations' privacy procedures, but instead refer to the right to carry out "investigations". While this can include demanding access to documents, or even conducting on-site inspections, it does not necessarily give them the scope to carry out full audits.

Privacy regulators tend to have different motivations for using privacy audits. While some view them as an enforcement or investigatory tool, others tend to regard audits as a proactive way to help organisations achieve compliance with the national law.

Dr Jan Willem Broekema, Commissioner of the Dutch Data Protection Authority, explained: "We perform audits specifically to enforce legislation." The Irish data protection authority, however, takes a different approach, and initiates its audits on a voluntary basis. "Privacy audits should not be seen as a threat, but as an aid to compliance," said Tom Maguire, Deputy Commissioner for Ireland's Data Protection Authority.

The UK has adopted a similar approach. Audits (referred to as assessments) are specifically mentioned in the Data Protection Act, but only in the context of the Information Commissioner's duty to promote "good practice". While the Commissioner has the power to carry out investigations into alleged privacy breaches, full audits can be carried out only with the consent of the organisation involved.

Even if auditing is used as a tool for "good practice", organisations have questioned whether it is in their best interests to voluntarily open up their privacy procedures to national regulators. The concern is that an audit carried out by a regulator could eventually lead to a barrage of enforcement notices for non-compliance.

Fortunately for organisations in the UK and the Netherlands, they do not have to wait to be audited by the national regulator as they can access their methodologies for their own internal or external audits.

Burden on regulators

Despite being regarded as an important compliance tool, data protection authorities carry out relatively few audits. In the case of Ireland it is just a handful, while France manages around 30 per year. There are exceptions to the rule, with some data protection authorities adopting a more rigorous approach to auditing. Dr Andrzej Kaczmarek, IT director at the Polish data protection authority, explained that his authority carries

out between 200-300 audits per year.

The overall low number is because audits are a drain on resources, taking up time, staff and money. For smaller countries with limited budgets and staff, carrying out a significant number of audits is just not feasible. The fact that regulators often spread their duties across a number of areas – including enforcement, education, consultation, and policy advice – makes it difficult to place a strong emphasis on any one particular area without neglecting the other duties.

Need for new initiatives

The challenge for data protection authorities is to promote the value of privacy audits, but without placing any further burden on themselves. The Dutch Data Protection Authority is currently developing an auditing scheme with the aim of providing an incentive for the business community to finance their own audits. The idea behind the scheme, explained Dr Broekema, is to encourage businesses to audit their practices for compliance, and then let them exploit the results as a commercial advantage by promoting themselves as a 'trustworthy' organisation.

The intention is to allow audited companies to display a privacy certificate that acknowledges their compliance with the law. As part of the scheme, the Dutch Data Protection Authority will establish an independent accreditation body responsible for approving data protection auditors. Accredited auditors would then be able to award the certificates to those organisations that have complied with the standards required. The certification scheme is expected to be up and running sometime during 2003.

The use of privacy certificates as generators for consumer trust is not a new concept. Organisations such as US-based TRUSTe provide online certification programmes which act as independent seals of approval for businesses' privacy practices. Privacy experts, however, have called into question the effectiveness and impartiality of these programmes. As far as the privacy campaigners are concerned, the fact that the likes of Amazon, DoubleClick and Microsoft – whose privacy practices have been pilloried by certain quarters of the IT media – are signatories to TRUSTe's seal programme, puts a question mark over the validity of the seal.

The Dutch approach, however, would see companies provided with a certificate that has received the stamp of approval from an independent data protection authority. This, argued Dr Broekema, would provide an added value above that of commercial certification schemes.

Dr Broekema admitted that some of the scheme's finer details still need to be worked out. For example, David Smith, Assistant Commissioner at the UK's Data Protection Authority, has raised the issue of how much compliance would be needed before a privacy certificate could be awarded. Will an organisation need to be 100 per cent compliant in order to receive a certificate?

> Businesses can exploit audit results as a commercial advantage by promoting themselves as a 'trustworthy' organisation.

In practice, that would be very difficult. So how about 98 per cent, or even 95 per cent? Where exactly should the line be drawn? If a privacy certificate is awarded for an organisation that is 95 per compliant, what about the 5 per cent of the business that is not compliant, argued Smith. That small area of weakness could lead to a legitimate complaint and effectively drag down the integrity of the certificate scheme.

The Dutch scheme is a good example of how regulators can provide incentives for businesses, and it will be interesting to see how successful it becomes. The scheme has provoked interest from other countries, and at an EU-wide level. Diana Alonso Blas of the European Commission's Internal Market Directorate, said that the Commission is "following this issue with a lot of interest," and regards such audit schemes as useful compliance tools.

A harmonised approach to auditing

The lack of harmonised privacy laws across the globe has raised enormous problems for multinationals when it comes to auditing. For example, an organisation may have audited its practices according to Dutch law, but what use would that be to its operations in Germany, or the UK for that matter? What would be of benefit to multinationals is an international standard auditing methodology. If the methodology is then approved by an international body, the European Commission in particular, then organisations can implement a recognised auditing standard without having to worry about varying the methodology to comply with the difference in national privacy laws.

The issue of auditing has been discussed on an international level by the European Committee for Standardization (CEN). The CEN's working group – the Initiative for Privacy Standardization in Europe (IPSE) – published a report in February this year, which concluded that an inventory of data protection auditing practices should be prepared that can assess best practice and the "extent to which the practice of data protection audit[ing] could benefit from standardisation." A meeting in Brussels on December 4th will discuss the next steps.

Business incentives?

Developing schemes for privacy auditing is one thing, but privacy regulators still need to come up with some convincing arguments if they are to persuade businesses that is it in their best interests. The corporate incentives fall mainly into two camps; meeting regulatory obligations and preserving consumer confidence and trust in the company brand.

Some sectors of US industry have strong regulatory incentives for conducting audits. Two US laws – the Health Insurance Portability and

Accountability Act (HIPPA) and the Gramm Leach Bliley Act – governing the healthcare and financial sectors – have prompted organisations to take a stronger interest in privacy audits. "HIPPA has huge implications for the industry of privacy auditing," said Ian Kahn of Transformative Knowledge Group, a US-based security and privacy auditing firm. The penalties for a breach of the HIPPA regulations, he explained, can result in both civil and criminal liability, which could potentially leave hospital administrators facing a jail sentence. "At one level," he continued, "just about every healthcare institution is going to have to do annual audits."

For companies wishing to implement a privacy compliance regime within their organisation, a privacy audit may well be the first step. A privacy audit of Colgate Palmolive, carried out by UK law firm Herbert Smith, enabled the company to identify the weaknesses in its systems and then draft the appropriate procedures and policies to overcome the problems.

Overall, compliance with legal obligations is not regarded as a high priority, mainly because of the lack of significant enforcement, explained Sandra Birkensleigh, national privacy director for the Australian arm of PricewaterhouseCoopers. In Australia, "because of the lack of financial penalties in the law, there is not a large demand" for privacy audits, she added.

It appears to be the need to maintain consumer confidence that is the key driver for implementing privacy audits. There is plenty of research to suggest that consumers care enough about their privacy to take their business elsewhere should they feel it is being infringed upon. While it may be hard to pin an actual dollar figure on the cost of a privacy breach, companies with well known brands and a reputation to maintain recognise the need to persuade their customers that they can not only provide an excellent service, but also offer effective privacy protection.

Earlier this year, a survey published by *Privacy & American Business* found that 62 per cent of the 1,529 people questioned said that an independent verification of an organisation's privacy policy would increase their trust. Professor Alan J Westin, founder of *Privacy & American Business*, said: "if American business wants to affect the attitudes and activities of today's consumer, independent verification is the single most preferred action to accomplish such a rise in trust."

Privacy policies may spell out what an organisation intends do with the data it collects, but sceptical consumers do not necessarily believe that businesses always practice what they preach. It is relatively easy for a legal team to draw up a standard privacy policy, but that does not guarantee that the rest of the organisation will stick to it. An independent privacy audit, therefore, not only gauges whether procedures are being adhered to, but can also act as a stamp of approval confirming that an organisation is doing what it says it is doing.

Microsoft appears to have realised this value. Following the investigation into its Net Passport service, the software giant is required to implement independent audits as part of its settlement with the Federal Trade Commission. However, Microsoft has indicated that it may continue with the audits on an indefinite basis. In a press statement, Brad Smith, senior vice president and general counsel at Microsoft, said that audits are seen as a "good tool to give partners and consumers assurance that the operations of the Passport service continue to meet a high bar."

Maintaining independence

Not all businesses take the view that employing independent auditors is the best approach. Some believe that internal auditors, who are more knowledgeable of the organisation's structure, will be able to spot areas of weakness that outsiders might not. Ian Kahn disagrees, saying that the task is often passed onto an already overburdened chief information officer who may not be able to devote the same diligence and expertise that an outside auditor might. Internal audits are "almost a guaranteed way to have bad outcomes," he said, "simply because it is another entrée on an already overfilled plate, and because it is not being done objectively."

CEOs need to be persuaded

With stronger regulation in place and more attention being placed on privacy issues by regulators and the media, the consequences of a privacy breach are becoming increasingly damaging. However, although they are on the increase, it appears that the vast majority of organisations still need to be convinced that a privacy audit is a spend worthwhile. Sandra Birkensleigh says it is extremely difficult to persuade a board of directors to provide the necessary finance. "There would still be a slant towards only spending the money in response to a crisis," she said. Of a similar opinion, is Ian Kahn. From his experience, companies' interest in privacy audits tends to be reactionary and is only aroused once a privacy incident has occurred. "It is not really considered a priority until someone has sued them for $10-15 million dollars," he explained. "Then it is a priority."

Comments from data protection commissioner's were taken from PL&B's International Data Protection Auditing Roundtable which took place at the Data Protection and Privacy Commissioner's 24th International Conference on September 9th.

The UK and Netherlands' data protection auditing frameworks can be found at: www.dataprotection.gov.uk/dpaudit/index.htm; www.cbpweb.nl/downloads/privacyauditframework.pdf

The Polish data protection authority has prepared a paper on its auditing practices. For a copy, contact Dr Adrzej Kaczmarek at: dif@giodo.gov.pl, or PL&B at: alan@privacylaws.com.

Websites of interest:
Herbert Smith – www.herbertsmith.com
Masons – www.masons.com
Transformative Knowledge Group – www.transformativeknowledge.com
PricewaterhouseCoopers – www.pwcglobal.com