

June 13, 2001

E-BULLETIN

PRIVACY ON PARADE

Stringent new privacy rules are shaping up as this year's business compliance headache. Josh Gliddon considers what they mean for companies and consumers.

The coming into effect of the Privacy Amendment (Private Sector) Act on December 21 will boost the level of privacy protection enjoyed by Australians. But along with greater rights come responsibilities – and those responsibilities fall squarely into the lap of business. Because of the complexity associated with compliance, Australian companies – and those operating in Australia – should think of the amendment as this year's GST or Y2K. Yet it's estimated that fewer than 30% of companies will meet their obligations in time.

All Australian businesses turning over more than \$3m a year will have to comply with the law, while those dealing with sensitive data, including medical information, are subject to even more stringent guidelines. The law may not prescribe penalties for those companies that don't meet the deadline, but liabilities will exist thanks to the grievance mechanism that could see breaches wind up in the federal magistrate's court. Non-compliance could also limit the ability of Australian companies to trade overseas, or even transfer information between different countries.

Until now, privacy laws have applied only to the public sector. The Privacy Act was introduced in 1988 in anticipation of the Australia Card, and while the identity card was abandoned the law survived. The amendment, introduced following pressure from the private sector, came in the wake of strict European Union privacy directives, the introduction of which caused a minor trade incident with the United States last year. This issue was eventually resolved through the use of a safe harbour clause that holds companies transferring information between the United States and EU to higher privacy standards than those mandated by American law. So far, 41 US companies, including giants such as Microsoft, have signed a safe harbour clause.

The amendment is not without its critics. Privacy advocates, including Irene Graham, chair of advocacy group Electronic Frontiers Australia, feel that the legislation doesn't go far enough. According to Graham, it is soft on the protection of children and doesn't measure up to global standards because penalties aren't enshrined by law. Additionally, the \$3m turnover baseline could exclude some companies that do handle sensitive information.

The EFA isn't alone in taking this position. The EU has described the legislation as inadequate, a move that led Attorney-General Daryl Williams to issue a statement saying that the EU didn't understand the Australian situation. Regardless of the bickering, the EU's critical stance could prevent Australian companies from doing business with their European counterparts. It's possible to avert this situation by doing as the law allows, and developing privacy guidelines that meet EU standards and comply with Australia's National Privacy Principles upon which the amendment is based.

There's a misperception that the amendment is somehow "internet" focused and although electronic information is an important consideration, the legislation is designed to be technology neutral. Bernard Hill, a barrister and privacy specialist for 90East, a security company charged with managing more than 30 major networks on behalf of the federal government, emphasises that the legislation applies to any information about a person, regardless of the way the information was collected, or the form in which it is stored. "The legislation applies to any information from which a person's identity could conceivably be derived," says Hill. "And that can include a person's opinion and other seemingly tangential information."

The amendment is based on the National Privacy Principles developed by the Privacy Commissioner. The core of the NPPs is that individuals must have the right to access information held on them. That right is enshrined in NPP6, which in turn builds upon NPP3, which claims for individuals the right to ensure that personal information held on them is accurate and up to date. "The rationale behind the law is to improve the trust relationships between individuals and companies," says Hill.

This right to access will open a can of worms. Individuals, except in limited circumstances – information collected before the introduction of the amendment is exempt, as is information deemed commercially sensitive – will have a right to access the information a company holds on them, and will have the right to have this information corrected if it is wrong. The law doesn't prescribe how individuals will gain access to their personal information, nor does it suggest methods for making that information available. These questions of access pose significant challenges for Australian business, but also provide opportunities for companies to ensure that their databases and procedures are up to date.

"Make no mistake, this legislation will be labour-intensive to comply with, and there's potential for individuals to use the [privacy] process to rightly or wrongly air grievances about a company," Hill says.

In order to comply, a company must advertise that individuals can have access to their personal information. The time within which a company must respond isn't mandated by law. However, the Privacy Commissioner has recommended that requests be met within two to four weeks. And although the amendment doesn't specify penalties for non-compliance, individuals will have the avenue of the federal magistrate's court open to them if they feel their privacy has been compromised.

Finally, there's a strict clause within the amendment regarding the transmission of personal information overseas. If the country that the information is being transferred to doesn't have laws in sync with Australia (and indeed with the EU privacy directives on which the legislation is based) then the company making the data transfer will find itself in breach of the law. Despite the lack of specified penalties, this has serious ramifications for companies operating across numerous jurisdictions.

"Consumer sentiment about privacy is quite legitimate," says a spokesman for the National Australia Bank. "We had long advocated a code that was in sync with those of the OECD. There's a good reason for this. Nearly half of our business is conducted across borders. We needed a law that would be consistent with practices overseas both now and in the future.

"We'll meet the deadline, but that's not to say there aren't challenges," he says. "We've not been allowed to amalgamate data – by law – even among our subsidiaries. So there's the challenge not just of compliance, but of making the law work for us and for our customers. Ultimately, we think that the benefits to be derived from the amendment aren't cost benefits. They're benefits that revolve around the customer."

The NAB isn't alone in taking that position. Ulysses Chioatto, national director, intellectual property and privacy at Deloitte Touche Tohmatsu, says that business shouldn't view the legislation as onerous. "Good privacy is good business. It increases the level of trust between individuals and organisations. Most marketing efforts are currently wasted. By ensuring greater privacy an organisation can, paradoxically, get to know their customer better and deliver a more appropriate level of service."

But getting there is going to be a challenge, and the challenge for business isn't, as it was with Y2K, simply a technical issue. "I'd estimate that only 20% of compliance issues relate to technology matters," says Chioatto. "The rest are policy and structural matters."

The key changes include the management of databases, including the access given to those databases by individuals inside and outside the organisation. Everyone that comes into contact – or could potentially come into contact – with personal information needs to be educated about their responsibilities. Security, therefore, needs to be increased company wide, and systems need to be given a thorough privacy audit. "You need to be able to track every single screen, in the case of a CRM system, that an employee views," says Steve Burke, general manager for IBM's Tivoli software division. (CRM, or customer relationship management, is a set of software applications and procedures designed to allow companies to – in theory – manage their interactions with customers across the phone, internet or in person.) "Those employees need to be made aware of their obligations."

It's not just employees. Everyone from the CEO down must understand that they have new obligations, and need to understand that non-compliance could pose a threat to the public image of the business, and perhaps even the ongoing viability of the organisation. For companies where their relationships with customers is the fulcrum upon which their business balances, compliance with the law is essential.

One way of addressing this is to install a chief privacy officer, or privacy tsar, within the organisation. "There needs to be discussion within a company about privacy," says Chioatto. "A CPO is needed to manage that discussion, to be the over-arching person that brings together the different jurisdictions within a company, such as marketing and human resources, to focus on the goal of privacy.

"A company needs to understand that privacy is good business," he says.

Material in The Bulletin is protected under the Commonwealth Copyright Act 1968. No material may be reproduced in part or in whole without written consent from the copyright holders.