
# The public face of privacy reform

In the age of Wikileaks, Edward Snowden's revelations about the USA's National Security Agency spying activities and phone hacking scandals galore, comes Australian law reforms that compels organisations to develop a policy around the collection, storage and retrieval of confidential information and report data breaches when they occur. But are Australian organisations ready for the legislation?

By Adeline **Teoh**
Correspondent

Compared to technology, legislation moves at a glacial pace. Parliament needs to balance the practicalities of implementing a new law against the need for legislation, then there's the process of asking for stakeholder input, and the subsequent debate and deliberation that occurs before the Bill comes into effect.

The Privacy (Enhancing Privacy Protections) Act 2012, due to commence on 12 March 2014, is on-trend with results from a survey conducted by the Office of the Australian Information Commissioner (OAIC) last year that revealed Australian attitudes towards online privacy. A majority of Australians (60 percent) indicated they had declined to deal with a company due to concerns regarding how their personal information would be used. It seems their concerns are well founded, with data breaches a common occurrence.

## Privacy in principle

When the privacy amendments come into effect, organisations will need to adhere to the new Australian Privacy Principles, which cover how entities must collect and hold personal information; the purpose for which they may collect information; how individuals may access and seek correction of their information; how individuals may complain about privacy breaches; and what to do if an entity is likely to disclose personal information to overseas recipient. The fine for non-compliance is up to $1.7 million per organisation, or $340,000 per individual.

Rob Livingstone, a fellow of the University of Technology Sydney Faculty of Engineering and Information Technology, who also runs his own IT advisory practice, says the amendments show the law has taken community attitudes seriously. It will also help organisations refocus on what controls they have including checking if software security controls and measures are up to a standard that would be defensible.

Michael Toms, ANZ Regional Director of information security company Clearswift, says good policy can't be broad, it needs to detail what information the organisation will collect and why. "If you have a clear policy and procedure on how you're going to deal with a person's information or another entity's information, if you can cover that in a

### In the dark

**More than one-third of Australian businesses and 73 percent of IT decision makers are unaware of amendments to the Privacy Act that will come into effect on 12 March 2014. The amendments require organisations to report data breaches to stakeholders or face a fine of up to $1.7 million for non-compliance.**

**Alarmingly, of the businesses surveyed, 24 percent suffered some form of data security incident in the past 12 months and 44 percent believe the source of the breach came from their own employees in the form of human error and personal devices in the work environment. Additionally, a further 20 percent of respondents say data breaches originate from ex-employees and 21 percent believe trusted partners such as customers or suppliers are the sources of breaches, which highlights the threat from the 'extended enterprise'.**

**Source: Clearswift's 'The Enemy Within' report (October 2013)**

meaningful way, I think you're on a very good path."

Despite the era it has taken for the privacy amendments to come to fruition, however, it turns out that there is still a significant portion of Australian organisations that are in the dark about the law. According to research conducted by Clearswift (see box above), 35 percent of Australian businesses and 73 percent of IT decision makers are unaware of the changes and what it might mean for their information gathering, storage and retrieval processes.

## When data leaks

"Data breach is when the confidentiality and the integrity of personal information held in trust by other organisations is compromised. That could include loss, corruption, unauthorised disclosure," says Livingstone.

Management of data involves a number of steps, from the secure collection and storage of information to its retrieval, a continuous process. "Essentially it's about implementing and maintaining the appropriate governance controls and security processes with the appropriate levels of ongoing integrity. It's not a one-off thing – it has to be embedded in the whole organisation."

Innocent leaks, such as when individuals disclose unsolicited information, need to be handled with care as well, adds Toms. "The entity must, within a reasonable period of receiving that detail, determine whether it could've been collected under the privacy principles. The unsolicited information [section] is important because what we will see is circumstances where you have to destroy data as well as collect, you can't just keep collecting stuff that's not core. If you're not meant to see that detail, you're probably better off not receiving it, or removing it from the information flow. Yes you're going to collect data, but what are you going to do about what you don't need?"

Where there's a huge challenge is in the notification of a breach. "The fundamental issue is to drive the proactive management of data breaches," says Livingstone of the amendments. "If there's a legal obligation to publicly report a serious breach of privacy, then it's a big disincentive for the organisation to sweep it under the carpet."

But requiring an organisation to alert its stakeholders to

"Reporting a data breach by an overseas outsourced provider is actually quite difficult," Livingstone warns. "An Australian organisation typically has no control over the actual operation of the business, they are relying on the terms of the contract and the penalties associated with that."

a data breach could lead to further attacks, Toms speculates. "When those kinds of breaches are posted online it actually formulates interesting research material for hackers. Posting those breaches may actually appeal to more capable people who have ideas of how to do that again."

Add the fact that two-thirds of breaches are not discovered until months after the incident and the majority by an external party to the leaker, according to Verizon's 2013 Data Breach Investigations Report, and the legislation starts to show some cracks.

Having a flag raised immediately when there's unauthorised access or misuse of data information is a key control issue, Livingstone says. Data breach notification should work like a burglar alarm; alert the breached organisation, which investigates and determines if the breach was genuine. If genuine, the organisation should notify the affected parties. "The issue of alerting is only one of a suite of good practice controls – prevention needs to play a part. Absolute guarantees are not feasible in this hyper connected world, but the issue of notification is an important step in the right direction."

## A global reach

The principles specifically make provision for the global nature of data collection. Any Australian organisation that outsources data collection or storage to an overseas entity needs to be aware that the overseas provider is also subject to this legislation. This includes offshore call centres and cloud computing providers. "If organisations are doing business in Australia, they have to detail to you how your data is being dealt with and protected if it's being held overseas," Toms points out.

"Reporting a data breach by an overseas outsourced provider is actually quite difficult," Livingstone warns. "An Australian organisation typically has no control over the actual operation of the business, they are relying on the terms of the contract and the penalties associated with that."

He says Australian organisations should not only draw up new contracts that explicitly include the new privacy principles, but should also conduct more thorough due diligence of overseas providers. "There are a whole lot of factors that should be considered where normal procurement process would be lacking. The legal side is important but it is no substitute for the appropriate level of due diligence to be done on that provider."

## Is it enough?

The legislation will provide more transparency to individuals about what information is being collected and why. "People are going to get a lot more exposure to where their information is going," says Toms. Unfortunately, it won't change the threat landscape, which he says is rapidly evolving.

Livingstone calls it an arms race between Governments and cyber criminals and says legislation alone is no guarantee of the maintenance and retention of trust between an organisation and an individual. One issue is budget cuts. "Organisations are keen to cut unnecessary costs and the attraction of cutting investment needed is a constant trade-off, especially if there has been no history of data breaches," he explains. "If it has never happened, why mitigate against it?" Meanwhile, cyber criminals are investing in more sophisticated attacks.

He maintains that organisations serious about maintaining their own internal governance processes should have breach notification as standard practice and use it like they would a burglar alarm. "That degree of rigour should be applied to all aspects of the organisation that are critical to its liability. And if the breach occurred through you, it's good practice to tell your customer so they know you are actively managing it." ■

### Your private checklist

Not sure if your business is ready? Follow this basic checklist.

- Read up on the amendment: www.comlaw.gov.au/Details/C2012A00197
- Develop a privacy policy based on the principles
- Create a procedure covering the collection of data, its storage and its retrieval
- Conduct a risk assessment for data breaches including all stakeholders – staff, customers, suppliers and overseas providers
- Implement a prevention strategy such as those recommended by the Australian Signals Directorate (www.asd.gov.au/infosec/top35mitigationstrategies.htm)
- Create a process for data breach notification.