

# Privacy reforms to cause industry shake-up

## New Australian privacy laws will lift the ICT security stakes

By Darren Pauli Sydney | Monday, 31 March, 2008

---

Australia could see its biggest data breaches yet when tough privacy laws clash with a lax security culture.

Amendments to the Privacy Act include a range of sweeping new powers allowing the Privacy Commissioner to enforce the mandatory reporting of new data breaches. It is a path New Zealand is looking increasingly likely to follow, after the Privacy commissioner here said there was a case for legislated disclosure last month.

Lyn Nicholson, a special counsel with Melbourne-based law firm Holding Redlich, says businesses may face a rude awakening when tough privacy enforcement laws arrive and clash with a blasé attitude to security.

"Online retailers not subject to significant regulation will be the ones hardest hit; their assumptions that a bit of security is enough will be tested," Nicholson says.

"We haven't had big data breaches in Australia and it is easier for companies to keep people quiet.

"Industry will react when someone has a big breach and is served a large fine."

The changes could see Australia heading down the US path where data breaches attract hefty fines and civil action, according to Nicholson.

She said the turning point will be after the prosecution of a high-profile privacy breach.

"I don't expect the Privacy Commission to start handing out draconian fines, but infringement penalties could be followed by civil action. Australians are not as aware as Americans of their privacy rights, but this will change when the new laws settle in."

An Australian Law Reform Commission (ALRC) discussion paper detailing 301 privacy reforms is expected to go to parliament in June after it was delayed past its March 31 deadline.

The reforms will be mandated after the paper and submissions have been discussed in parliament, which industry experts say will be no earlier than 2009.

Businesses can already be dealt harsh fines for data breaches under a clause in the Trade Practices Act.

The clause can be enforced similarly to the case against online apparel retailer Life Is Good, which was ordered by the US Federal Trade Commission (FTC) in January to undergo external security audits for the next 20 years.

The FTC alleged the company stored credit card information indefinitely on its computers, without using proper encryption software or sufficient access controls. The FTC also claimed the company violated federal law by allegedly making security claims on its website that were false.

Parliament will most likely pass the general provisions of the new privacy laws first, followed by components pertaining to sensitive records and credit reporting.

The Act will be based on the best parts of the US and UK laws coupled with industry codes of conduct such as those used in New Zealand, according to Nicholson.

The reforms will likely give the Privacy Commissioner new powers to amend legislation to facilitate emerging technologies including biometrics, data warehousing of customer information and high profile breaches of sensitive data.

Andrew Hayne deputy director of policy for the Office of the Privacy Commissioner said the codes are designed to add specificity to the current Act which has been attacked for its weak non-specific structure.

"The requirement [for notification of privacy breaches] should not be an unreasonable burden on business and it should not result in alarmous [sic] notification," Hayne said.

The reforms will merge Australia's dualist IPP and NPP privacy laws, which mandate similar policies for federal and state organisations, into a single Act to reduce complexity.