

Consumer protections gap to widen

PUBLISHED: 24 Jan 2012 PRINT EDITION: 24 Jan 2012

Brian Corrigan

Australia looks set to fall further behind other advanced economies in championing the rights of consumers who have had personal details exposed by corporate security breaches.

European regulators will this week lay out plans to force companies into notifying customers of data breaches within 24 hours as part of broader efforts to strengthen existing consumer protection legislation.

Data breach notifications are managed at a state level in the United States so approaches vary wildly, but many have had legislation in place for almost a decade.

Company disclosures suggest it is a growing problem locally. The Office of the Australian Information Commissioner's first annual report, published late last year, said it had received 56 data breach notifications in 2010-11. This was up 21 per cent on the previous year.

Yet consumers might never know that their financial and other details have been exposed because Australia relies on voluntary notifications. That means businesses are under no obligation to inform the Privacy Commission or their customers of data breaches.

The Australian Law Reform Commission recommended introduction of mandatory breach notifications four years ago. A spokeswoman for the Attorney-General's Department said yesterday that it was working through the ALRC's recommendations in stages and would get to data breach notifications "in due course".

In a string of high-profile incidents that brought data breaches to the attention of company boards, personal customer details have been hacked by activists to highlight poor security. Sony has been the most prominent victim, with two separate breaches exposing personal details of more than 100 million customers.

Australian Privacy Foundation chairman Roger Clarke said data breach notifications should have become mandatory 10 years ago to "embarrass the hell out of those organisations that leak like sieves".

He criticised regulators and major political parties for failing to act. "Both sides of politics have been in the thrall of national security extremism for the last decade and civil law doesn't get a look in," Dr Clarke said.

"Information law was handed back to the Attorney-General's office at the end of last year and that is a death knell for any meaningful developments in privacy. Government is hostile to privacy protections."

Lyn Nicholson, a special counsel with law firm Holding Redlich, said it was difficult for businesses to do anything within 24 hours because they needed time to work out the best steps to take. "Consumer advocates can say 'let's notify within 24 hours' but you need some time to investigate the nature of the breach and the extent," she said. "It needs to be accurate. If you don't allow people time to work out that what they're telling you is correct, that's unreasonable."

Ms Nicholson said progress was being made towards updating privacy legislation although she admitted it had been a long process. She noted that a lot of internet privacy issues were dealt with by telecommunications laws, which meant plenty of consumer protections were in place.

Dr Clarke said organisations should face criminal sanctions for serious breaches. "Let's put requirements on organisations to have appropriate levels of security and apply standards that are well known," he said.

The Australian Financial Review

Related News

People [Roger Clarke](#)

Topics [Technology/Corporate & Government IT](#)



Create an alert

Click on the links below to create an alert and receive the latest news as it happens

People [Roger Clarke](#)

Topics [Technology/Corporate & Government IT](#)

KEY POINTS

- n Businesses are under no obligation to inform the Privacy Commission or their customers of data breaches.
- n The Australian Law Reform Commission recommended introduction of mandatory breach notifications four years ago.