HERBERT SMITH FREEHILLS

MANDATORY REPORTING OF DATA BREACHES ON THE HORIZON

10 November 2015 | Australia, Brisbane, Melbourne, Perth, Sydney
Legal Briefings

The Australian Government has indicated that it will introduce mandatory data breach notification laws in 2015. Mandatory data breach laws have been in the pipeline since 2009 following Australian Law Reform Commission recommendations.

IN BRIEF

- The Australian Government has indicated that it will introduce mandatory data breach notification laws in 2015.
- Mandatory data breach laws have been in the pipeline since 2009 following Australian Law Reform Commission recommendations.
- The Turnbull Government may introduce its own legislation following *Privacy Amendment (Privacy Alerts) Bill 2013* stalling in the senate.
- Voluntary notifications of data security breaches are on the rise.

SUMMARY

In March this year, Attorney-General George Brandis and the then federal Communications Minister Malcolm Turnbull released a joint statement indicating that the federal government intends to introduce a mandatory data breach notification scheme by the end of 2015.[1] The statement came in the Government's response to a report by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The report mainly dealt with Australia's proposed 'data retention' laws, which grants the Government controversial new powers to collect and retain metadata for terrorism and criminal investigation purposes.

At present, while there are obligations in the *Privacy Act 1999* (Cth) to keep personal information secure, notification of a breach is voluntary and companies are simply encouraged to follow the Office of the Australian Information Commissioner's (OAIC's) guide.[2]

THE LEAD UP TO THE PROPOSED CHANGES

In 2009 the Australian Law Reform Commission (ALRC) recommended that the federal government introduce mandatory data breach laws. This was one of 295 privacy reform recommendations the ALRC released; the government has answered 197 of the recommendations in October 2009 but the *Privacy Act* has yet to be updated.

In March 2013, Senator Lisa Singh proposed as a private member's bill the *Privacy Amendment (Privacy Alerts) Bill 2013*, which aimed to amend the *Privacy Act 1988* (Cth). The suggested laws, which were scheduled to commence on 12 March 2014, commanded notification of serious data breaches that would result in 'a real risk of serious harm'. However, the bill never passed following initial opposition by the Attorney-General's department. It now appears more likely that the Turnbull Government will introduce its own legislation.

WHAT WOULD MANDATORY REPORTING INVOLVE?

The proposed changes contained in the original *Privacy Amendment (Privacy Alerts) Bill 2013* required the Privacy Commissioner and 'significantly affected individuals' to be alerted about 'serious data breaches' when:

- personal, credit and/or tax file information 'held' by an entity had been subject to unapproved access or disclosure, including when the loss of such information could compromise its security, in breach of the data security obligations in the *Privacy Act* (see Australian Privacy Principle 11.1), and
- the entity believed on reasonable grounds that the breach was 'serious' because it would result in a 'real risk of serious harm' to the individual. A 'real risk' is defined as a risk that is not a remote risk and 'harm' includes psychological, physical, reputational, economic or financial harm.

While the Turnbull Government may propose different thresholds, any mandatory reporting scheme will importantly not be limited to telecommunications service providers and will represent a significant new compliance burden on all businesses. The changes will undoubtedly see an increase to the overall cost to companies when handling data security incidents.

VOLUNTARY REPORTING ON THE RISE IN THE ABSENCE OF LEGISLATIVE REFORM

The Information Commissioner, Timothy Pilgrim, identified that in 2013-2014 there was an increase in the number of voluntary data breach notifications. In line with the OAIC's voluntary data breach notification guidelines, a greater number of entities chose to notify the OAIC of a data breach incident despite not yet having any legal requirement to do so. A total of 71 notifications were made, representing an increase of 16%.[3] The trend highlights the value that businesses are placing on their customers' data according to the Information Commissioner. *"Notification demonstrates that an entity respects their customers' personal information and thereby strengthens the trust equation in the relationship"* he said.

This article was written by Caitlin Cross, Solicitor, Melbourne.

ENDNOTES

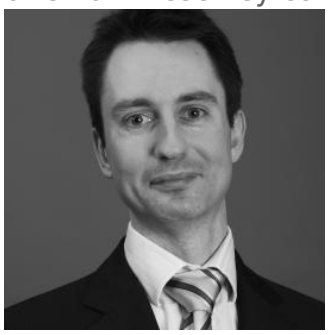
1. Attorney-General for Australia, The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 3 March 2015.

2. Office of the Australian Information Commissioner, Data Breach Notification: A guide to handling personal information security breaches.

3. Office of the Australian Information Commissioner, *Message from the Privacy Commissioner, Timothy Pilgrim – Annual Report 2013-14*.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

LEGAL NOTICE