HERBERT SMITH FREEHILLS

NEW PROPOSAL FOR MANDATORY REPORTING OF DATA BREACHES

09 December 2015 | Australia, Brisbane, Melbourne, Perth, Sydney
Legal Briefings

The Federal Government has released an exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.

IN BRIEF

- The Bill will require Federal Government agencies and most businesses with a turnover above $3 million to notify 'serious data breaches' to affected individuals and the Australian Information Commissioner.
- The Government has invited public submissions on the proposed Bill which must be received by 4 March 2016.

THE DRAFT BILL

The Federal Government has released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*.[1] The Bill is designed to add a new data breach notification regime to the *Privacy Act 1988* (Cth). Public comment has been invited before the Bill is introduced in parliament in 2016.

As with many other requirements under the Privacy Act, serious and repeated breaches will be subject to enforcement actions including civil penalty orders of up to $1.8 million.

THE LEAD UP TO THE PROPOSED CHANGES

In 2008 the Australian Law Reform Commission (**ALRC**) recommended that the Federal Government introduce a mandatory data breach notification scheme that would apply to data breaches which create a 'real risk of serious harm' to affected individuals. The previous Government introduced a mandatory data breach notification bill in 2013 based on the ALRC recommendation, but the bill did not pass during the life of that parliament.

In March this year, the Federal Government announced its intention to introduce a mandatory data breach notification scheme by the end of 2015.[2] The timing and context of this announcement appeared to be a concession to public concerns around the introduction of Australia's 'data retention' laws, which grant the Government controversial new powers to collect and retain communications metadata from telecommunications providers for terrorism and criminal investigation purposes.

At present, while there are obligations in the Privacy Act 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.[3] The OAIC also considers that having a data breach response plan is one way to help satisfy security obligations under the Act. Mandatory breach notification is required only in the event of unauthorised access to eHealth information under the *Personally Controlled Electronic Health Records Act 2012.*

WHAT WOULD MANDATORY NOTIFICATION INVOLVE?

The draft Bill is similar to previous proposed legislation dealing with data breaches, in that it would require the Australian Information Commissioner and 'affected individuals' to be alerted about 'serious data breaches'.

A data breach arises where there has been unauthorised access to, or unauthorised disclosure of, personal information, certain credit information or tax file number information, relating to one or more individuals. As in overseas jurisdictions, there is a threshold requirement to notification that there must be a 'serious data breach' which will occur where there is *a real risk of serious harm to the individual* to whom the information relates. In addition, the draft Bill provides for regulations to specify particular types of situations as serious data breaches even if they do not reach the threshold of a real risk of serious harm.

Notification would be required where there are reasonable grounds to believe that a serious data breach has occurred. If an entity suspects but is not certain that a serious data breach has occurred, the entity has 30 days to assess if notification is required. If an entity fails to detect a serious data breach that they should be aware of, they will be in breach of their notification obligations.

Entities are required to take all reasonable steps to notify affected individuals, and where that is not practicable to publish a notice on its website. It is not clear whether the fact that an organisation has been contacted by someone to advise of the potential for a data breach is itself a notifiable event.

The notice should include a description of the breach, the types of information affected, and recommendations as to the steps individuals should take in response to the breach.

WHAT DOES IT MEAN FOR YOUR BUSINESS?

This mandatory reporting scheme set out in the draft Bill will not be limited to telecommunications service providers. It will apply to all entities who are bound by the *Privacy Act*, namely Federal Government agencies, private sector organisations with an annual turnover above $3 million (and their related companies) and some others. This will represent a new compliance obligation for business and the changes will undoubtedly see an increase to the overall cost to companies when handling data security incidents. Arguably, the new obligations will also have the effect of stimulating companies to do more to prevent data breaches occurring and to detect them early, in order to minimise the likelihood that they will need to make a data breach notification, which can give rise to unwanted publicity.

In its latest annual report, the OAIC reported receiving 110 voluntary data breach notifications for 2014-15, an increase of 64% on the previous year.[4] The Ponemon Institute's latest Cost of Data Breach Study for Australia found the average cost of a data breach for companies in the study to be $2.8 million, including the cost of lost business and customer churn.[5]

Businesses who fail to comply with their notification obligations face investigations and enforcement action including potential penalties for serious or repeated infringements and the possibility that the OAIC will seek enforceable undertakings. The fact that a business was not aware of their serious data breach does not relieve them from liability if they reasonably should have detected the data breach.

The Government has invited public submissions on the proposed Bill which must be received by 4 March 2016. Some of the matters entities may raise in submissions include the scope of exceptions, timing requirements, liability for undetected breaches, compliance costs, the types of information covered, the Information Commissioner's role and the adequacy of existing mechanisms.

This article was written by Lesley Sutton, Partner, Sydney and Kaman Tsoi, Special Counsel, Melbourne.

ENDNOTES

1. Serious data breach notification.

2. 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.

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

4. Office of the Australian Information Commissioner, Annual Report 2014-15.

5. Ponemon Institute, Cost of Data Breach Study Australia 2015.

KEY CONTACTS

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

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

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

TONY JOYNER
LEAD PARTNER – TMT, PERTH
+61 8 9211 7582
Tony.Joyner@hsf.com

LEGAL NOTICE