University of New South Wales Law Research Series

AUSTRALIA'S DATA BREACH NOTIFICATION BILL: TRANSPARENCY DEFICITS

GRAHAM GREENLEAF

(2016) 139 *Privacy Laws & Business International*

Report 18-19, 30 January 2016

[2016] *UNSWLRS* 54

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: : http://www.ssrn.com/link/UNSW-LEG.html

Australia's data breach notification Bill: Transparency deficits

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2016) 139 *Privacy Laws & Business International Report*, 18-19

30 January 2016

Australia's conservative (Liberal/National) coalition agreed to introduce a mandatory data breach notification (MDBN) scheme, as part of the political trade-off to obtain parliamentary passage of its data retention law in 2015.[1] It accepted a recommendation to do so by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), but made no commitments concerning the content of the Bill. MDBN legislation had previously been recommended by the Australian Law Reform Commission's (ALRC) report *For Your Information: Australian Privacy Law and Practice* (2008), and had been the subject of a Bill by the previous Labor government in 2013 which did not obtain passage during its term.

The government released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill* in December 2015, seeking submissions on it by 4 March 2016.[2] The draft Bill's MDBN scheme would commence 12 months after the Bill receives Royal Assent, so businesses will have at least a year to prepare following passage. The Bill will amend the *Privacy Act 1988*, and section references given here are to that Act as it would be when amended.

A 'serious data breach'

The basis of the Bill is that notification to the Australian Information Commissioner ('Commissioner'), and to affected individuals, would be required when there was a 'serious data breach'. Such a breach can occur where unauthorized access or unauthorized disclosure of privacy-relevant information puts one or more individuals who the information is about at 'real risk of serious harm'. It can also occur where loss of relevant information could lead to such unauthorized access or disclosure.

Scope of the Bill

Some limitations on the Bill's scope need careful consideration. The 'privacy-relevant information' that must be accessed or disclosed is information in one of the categories protected by Australia's *Privacy Act*: personal information; credit reporting information; credit eligibility information, or tax file number information. In addition, all 'retained telecommunications data' which ISPs and others are required to retain under the data retention law is defined to be 'personal information'. Information which is *not* covered by the Privacy Act (and therefore excluded unless it is held by an ISP etc) includes information held for employment purposes.

---

[1] Graham Greenleaf 'Going Against the Flow: Australia Enacts a Data Retention Law' (2015) 134 *Privacy Laws & Business International Report*, 26-28. The data retention law is the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.

[2] See: Australian Attorney-General's Department *Serious Data Breach Notification* <https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx>

The entities that will have MDBN obligations are also only those covered by the Privacy Act, which excludes in most cases businesses with a turnover of less than A$3M per annum (the so-called 'small business' exemption), employers in relation to employment information, media organisations, political parties and so on. However ISPs and other entities with obligations under the data retention law are included whether or not they would otherwise come under the Privacy Act. Federal government agencies are covered (significantly excluding those exempt from the Privacy Act), but not those of State, Territory or local governments.

Triggering notification: a 'real risk of serious harm'

The Bill sets out factors to be considered in deciding whether an access, loss or disclosure cases a 'real risk of serious harm', including factors relating to its subject matter, sensitivity, intelligibility (eg whether encrypted), protective measures, likely recipients, nature of likely harm, and mitigation of damage undertaken (s26WB(3)). Harm is given a very broad definition (s26WF), and 'real risk' means a risk that is not a remote risk (s26WG).

Once a regulated entity is aware, or ought reasonably to be aware, of reasonable grounds to believe that there has been a serious data breach, it must, 'as soon as practicable', (a) give a statement detailing the breach to the Commissioner and (b) take reasonable steps to notify each individual to whom the information relates. However, if it is not practicable to so notify individuals, the entity can publish the statement on its website and take reasonable steps to publicise its content (s26WC(1)). Where the Commissioner is satisfied that it is in the public interest to do so, she or he may give an entity a written exemption from its obligations under s26WC(1), but there is no requirement that the Commissioner make such exemptions public.

The Commissioner may of its own volition order an entity to undertake any of these various means of notification (s26WD).

Remedies under the Privacy Act

If an entity contravenes section 26WC or 26WD, 'the contravention is taken to be an act that is an interference with the privacy of an individual' (s13(4A)). These words mean that if an entity fails to comply with any of its notification requirements in accordance with the Act, data subjects who suffer damage can seek compensation or other remedies from the Commissioner. In effect, this means that the MDBN obligations is like an additional Australian Privacy Principle (APP). This is one of the best features of the Bill.

In flagrant cases, breach of the MDBN obligations could also potentially expose an organisation to civil penalty provisions for 'serious' or 'repeated' breaches.[3] The Commissioner must apply to the Federal Court or Federal Magistrates Court, for such a finding. The civil penalty is determined by the court, to the maximum of up to AUD$1.7 million (1.15 million euros) for companies, or up to AUD$340,000 (230,000 euros) for individuals.[4] In determining the amount of civil penalty, the court may consider all relevant matters including any loss or damage resulting from the breaches, which could be very significant if major data breaches are not notified.

Deficiencies – Stunted scope, transparency deficits

While a detailed assessment of the Bill would criticise additional aspects, two deficiencies stand out. The first is the unjustifiable wholesale exemption of organisations otherwise exempt from the Privacy Act. While the position of criminal investigative and security

[3] See G Greenleaf 'Privacy enforcement in Australia is strengthened: gaps remain'(2014) 128 *Privacy Laws & Business International Report* 1-5

[4] For section 13G, 2,000 penalty units (for individuals), or up to five time that for a corporate defendant.

agencies may require special consideration, small businesses, employers, media organisation and political parties do not require any special protection from MDBN obligations. They can be subject to these obligations without any necessity for the whole question of their exemptions from the Privacy Act being re-opened.

Second, as was the case with its 2013 predecessor, the Bill does not require that the Commissioner must publish on its website all of the statements it receives about serious data breaches, and retain them there for future reference. Unless such aggregation and publication occurs, many MDBN statements will never come to public attention, unless individuals who receive such statements make them public. Even if the statement is required to be published on a organisation's website, or a newspaper (because the organisation cannot inform all data subjects of the breach), it will soon be removed from the website, and newspaper notifications are easily missed at the time they occur. In short, MDBN statements will often not be publicly known at the time, and will not be findable permanently after the event, nor searchable in the one location.

All MDBN statements should be able to be browsed and searched, permanently, on the Commissioner's website. Interested parties including both the media and civil society organisations (and not only the Commissioner) would then be better able to identify any recurrent aspects of breach notification, including which agencies or companies are involved. This is also likely to have a deterrent effect on agencies and companies, inducing them to improve their security. It is also important to support the right of data subjects to make complaints and seek remedies against companies and agencies they suspect have not carried out their MDBN obligations, for which purpose they must be able to find with certainty whether or not a company made a MDBN statement. The cost implications of the Commissioner providing such a database are negligible, because MDBN statements will already be required to be made to the Commissioner in a standard form.

The Commissioner's website should also list the fact of applications for exemptions (anonymised where necessary on national interest grounds), and the result of such applications, given as much detail as is consistent with national interest. This will at least partially prevent the intended benefits of transparency that MDBN is supposed to serve from being defeated, and will act as a partial deterrent against such secrecy being sought.

The Bill should require these practices, but the Commissioner could also announce prior to its enactment that he will follow such a policy. A reform based on the need for notification of data breaches should not include such conspicuous transparency gaps.