Mandatory Notification of Data Breaches - Proposed to be Introduced in 2015
By Mick Coleman and Lisa Ptasznik

1 Background
1.1 Safeguarding information has become a complex task for organisations operating within global information networks, as it invariably exposes them to new security risks.
1.2 Currently, Australia has a process for voluntary reporting of data breaches to the Office of the Australian Information Commissioner, but no obligation mandating organisations to report data breaches to regulatory agencies or affected individuals.
1.3 The lack of oversight and secrecy around data breaches makes it difficult to generate reliable statistics about the nature and quantity of these incidents occurring across the Australia.
1.4 A key argument in favour of mandatory data breach notification is that it can give people the opportunity to reduce the impact of data security breaches, such as by cancelling credit cards or changing account passwords, and it can increase public confidence in the handling of consumer information.
1.5 Critics counter that data breach notification laws negatively impact businesses, both in compliance costs and unnecessarily frightening customers, particularly if reporting thresholds are low. An exposed data leak will likely have a negative impact upon consumer confidence in a breached organisation, as well as its brand and bottom line.
1.6 By enacting mandatory data breach notification laws, the Australian Government would enable business owners, consumers, law enforcement agents and policy makers to gain a more accurate picture of the data security breaches occurring each year.

2 How do data breaches happen?
2.1 Data breaches can occur in many ways.
2.2 Unauthorised access can occur as a result of a malicious breach of the secure storage and handling of that information (hacker attack or inadvertent publishing online), accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information (staff member mistakenly providing information to the wrong person), or otherwise.
2.3 The 2013 Ponemon report showed that organisations say:
   a. the root cause of 43% of data breaches was malicious or criminal attacks;
   b. 33% of breaches involved negligent employees or contractors; and
   c. 24% of breaches were due to IT and business process failures.

3 Current Australian Position
3.1 Australia does not currently have mandatory data breach notification laws. However, the Privacy Commissioner, who is part of the Office of the Australian Information Commissioner (OAIC), encourages notification by entities in accordance with the OAIC’s voluntary guidelines, entitled the ‘Guide to Handling Personal Information Security Breaches’ (available on the OAIC website).
3.2 The goal of the voluntary guidelines is to enhance security whilst encouraging and fostering transparency about the privacy practices of Australian organisations.
3.3 While there are obligations in the Privacy Act 1988 to keep personal information secure from mishandling and illegal access, there is no requirement for agencies and organisations to notify individuals, regulators or law enforcement agents about data breaches.
3.4 This means that while APP entities are obligated to minimise the likelihood that personal information within their possession could be compromised, they are not required to notify any individual or agency in the event of an actual security breach.

3.5 In March 2014 Lisa Singh, Tasmanian Labor Senator and parliamentary secretary to the Shadow Attorney-General Mark Dreyfus, re-introduced proposed legislation, the Privacy Alerts Bill 2014, which governs mandatory notifications for companies suffering a data breach.

3.6 The text of the Privacy Alerts Bill 2014 is identical to the Privacy Alerts Bill 2013, which failed to be heard on the last day of sitting before the September 2014 federal election.

3.7 Under the proposed Bill, an organisation would have been required to notify the Commissioner in the event of a serious breach, outlining among other things, the details of the serious breach; the compromised information; and any remedial steps that victims should take.

3.8 The Bill also requires the breached entity to notify each affected individual as soon as practicable with the following information: the identity and contact details of the breached entity; a description of the data breach; the kinds of information concerned; recommendations about the steps that individuals should take in response to the data breach; and any other information specified in the regulations.

3.9 The breached entity must provide this information directly, or take reasonable steps to notify the individual, or, if this is not possible, publish a copy of the statement on its website and in each state via newspaper publication.

4 Parliamentary Joint Committee on Intelligence and Security (PJCIS) Report

4.1 The PJCIS is appointed under section 28 of the Intelligence Services Act 2001 and its current membership is set out in the table below.

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Mr Dan Tehan MP</td>
<td>Liberal Party of Australia, Wannon VIC</td>
</tr>
<tr>
<td>Deputy Chair</td>
<td>Hon Anthony Byrne MP</td>
<td>Australian Labor Party, Holt VIC</td>
</tr>
<tr>
<td>Member</td>
<td>Senator David Bushby</td>
<td>Liberal Party of Australia, TAS</td>
</tr>
<tr>
<td>Member</td>
<td>Hon Jason Clare MP</td>
<td>Australian Labor Party, Blaxland NSW</td>
</tr>
<tr>
<td>Member</td>
<td>Senator the Hon Stephen Conroy</td>
<td>Australian Labor Party, VIC</td>
</tr>
<tr>
<td>Member</td>
<td>Hon Mark Dreyfus QC, MP</td>
<td>Australian Labor Party, Isaacs VIC</td>
</tr>
<tr>
<td>Member</td>
<td>Senator David Fawcett</td>
<td>Liberal Party of Australia, SA</td>
</tr>
<tr>
<td>Member</td>
<td>Mr Andrew Nikolic AM, CSC, MP</td>
<td>Liberal Party of Australia, Bass TAS</td>
</tr>
<tr>
<td>Member</td>
<td>Hon Philip Ruddock MP</td>
<td>Liberal Party of Australia, Berowra NSW</td>
</tr>
<tr>
<td>Member</td>
<td>Senator John Williams</td>
<td>The Nationals, NSW</td>
</tr>
</tbody>
</table>

4.2 The Government announced on 7 April 2015 that it supports the recommendation by the PJCIS, in its report on the controversial Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015, to introduce mandatory notification of data breaches by the end of 2015.

4.3 The stated reason was the need to provide strong incentives for telecommunications and internet service providers to implement robust security measures to protect data affected by the new metadata retention regime.

4.4 The PJCIS considered it appropriate that all telecommunications and internet service providers, including those that would not otherwise be bound by the Privacy Act, be subject to either the Australian Privacy Principles or other binding rules of the Privacy Commissioner.

4.5 The PJCIS noted in its report that a mandatory data breach notification scheme would be an effective mitigation strategy for those affected by a data breach.

4.6 Australia’s Privacy Commissioner Timothy Pilgrim responded,

“I welcome the Government’s support for a mandatory data breach notification scheme. Data breach
notification can increase consumer trust and mitigate against reputational damage. It is an important step to further protect the personal information of Australians.”

4.7 Although this issue is addressed by the Privacy Alerts Bill 2014, the Government has indicated it will introduce new draft legislation for consultation.

5 United States and Mandatory Data Breach Notification

5.1 California led the world in mandating notification following the 2005 ChoicePoint incident where ChoicePoint compiled and sold data on individuals to companies conducting background checks. Posing as a customer, fraudsters purchased from ChoicePoint the individual details of 163,000 individuals, resulting in 800 cases of identity theft.

5.2 Illustrating the enormous compliance effort that accompanies cross-jurisdictional activity, ChoicePoint is reported to have struck settlements with 43 US States. 47 States have followed California’s lead in legislating individually to mandate notification.

5.3 Other US jurisdictions contemplating the introduction of mandatory data breach notification have come to a range of different landings on related issues including:
   a. What is the test for what constitutes a security breach?
   b. Whether harm is an element, and if so what the test is?
   c. Whether the type of personal information required to be notified is co-extensive with personal information as generally governed by the regime, or something narrower?
   d. Who must be notified? When? By what means?
   e. What information the notification should include?
   f. What are the consequences for failing to meet these obligations?
   g. Should there be a punitive element as well as an administrative sanction?

5.4 Across the US, about half the States adopted the California model, while half adopted other models and an attempt at a Federal regime has made no progress to date.

5.5 Opponents in the US to mandatory breach notifications have criticised the regime noting that:
   a. mere “acquisition” by a third party is too low a bar to warrant reporting, demanding a response regardless of realistic prospect of use of the information, let alone harm;
   b. over-reporting of breaches has inured recipients whose first instinct is to see corporate communications as junk-mail – “boy who cried wolf” syndrome;
   c. focussing on “reputational sanctions” as opposed to “harm minimisation” has meant plenty of public recrimination but little practical effect (identity theft reduced by a mere 1.5% in States with mandatory notification compared to States without); and
   d. the exemption for encrypted information has encouraged encryption as intended but seems unlikely that all encrypted information is harm-proof.

6 European Union and Mandatory Data Breach Notification

6.1 The European Union has followed a similar path to the US.

6.2 The ePrivacy Directive of 2002 is a set of principled statements applying to all States.

6.3 National Parliaments like Germany and Spain passed their own mandatory breach notification laws, which however are over-ridden by European Parliament laws.

6.4 The European Parliament adopted an ePrivacy Directive in 2009, applying only to the electronic communications sector.

6.5 A supplementary Citizens Rights Directive also took effect in 2009, again applying only to electronic communications.

6.6 States had to bring their national laws into conformity by 2011.

6.7 Some features of the EU mandatory data breach notification regime:
   a. Covers “personal data” which is broadly defined to include “any information relating to an identified or identifiable natural person” and including traffic data relating to a person.
   b. Breach is also broadly defined to cover any unauthorised access in connection with the provision of
a public communications service.

c. Blanket duty to notify the national authority about any breach, regardless of harm.

d. More qualified duty to notify the affected individuals, where the breach is likely to adversely affect the personal data or privacy of the individual. **NOTE:** This qualification is supposed to avoid the US problems of over-notification, and reticence to report to authorities by offering a less public avenue. However, the authority can over-rule and demand individual notification.

e. Notification is not required if the company can show it has appropriate defence mechanisms such as encryption but this is not a complete defence as it is in the US.

6.8 A new **EU Cybersecurity Directive** proposed to become law in 2015-16 remains in negotiation between the European Parliament, European Commission, the Council of the EU and member states. If enacted, it would extend mandatory breach reporting beyond the communications sector to a yet-to-be-agreed set of “market operators” such as critical infrastructure operators, social media companies, government entities, energy suppliers, e-commerce platforms, internet-application stores and freight services.

7 **Next Steps**

7.1 The Australian Government’s pledge to introduce mandatory data breach notification by the end of 2015, coupled with the recent release by ASIC of its Cyber Resilience Health Check Report, reiterates the need for affected organisations to review their cyber security and cyber resilience plans.

7.2 The Government has indicated it will introduce new draft legislation dealing with mandatory data breach notification for consultation this year. At this stage the Government has not indicated how its new draft legislation will differ from the **Privacy Alerts Bill 2014**.

7.3 While mandatory reporting will not be confined to the telecommunications sector, telcos have a particular vulnerability following the recent data retention laws. Given that metadata may be commercially sensitive, there is a risk that the metadata retention obligation will unintentionally create a ‘honeypot’ for cyber-attacks by third parties.

7.4 The following practical steps are a useful starting point:

a. conduct a contractual review to determine the allocation of risks and responsibilities between your company, clients and third party providers;

b. identify the critical data, systems and services for which your organisation is responsible, with particular emphasis on personal information that is likely to be impacted by the amendments to the privacy laws or potentially attractive to hackers;

c. ensure employees are appraised of your cyber resilience plan and invested in its ongoing success;

d. cyber-attacks are no longer the domain of the IT department and executives should make it their business to understand antivirus software, firewalls, data encryption and hacking risks.

7.5 While the development of a cyber-resilience plan is crucial, there is no foolproof system for protecting your organisation from the threat of a cyber-attack, and organisations may also wish to consider the benefits of a specialist cyber risk insurance policy.

8 **Contacts**

Mills Oakley is a leading Australian law firm.

Our Corporate Advisory group can assist with submissions, advisory and notification work for companies affected by Australia’s privacy law framework.

**For more information, please contact:**

**Mick Coleman**  
Special Counsel  
T: +61 3 9605 0060  
E: mcoleman@millsoakley.com.au