10 Reasons why an Australian data breach notification law won’t make any difference

Having been on the drawing board since 2008, it is entirely possible that at some stage in the next two years, Australia may get its own version of a data breach notification law. But, assuming a law similar to the draft legislation issued for consultation in December 2015 is passed, will it make any real difference? This article argues that, for a number of reasons, the introduction of the proposed data breach notification law in Australia is unlikely to have any real impact on either the risk of harm to Australians or the security practices of the organisations affected by the law.

Key take-aways
The passage of the data breach notification amendments is unlikely to have any impact because:

1. There is no evidence of real change in either the extent of identity theft or improved information security practice in those U.S. States with data breach notification laws
2. The proposed law includes the sort of provisions found to be least effective in other jurisdictions
3. Resource restrictions will constrain both the compliance focused and enforcement activities of the Australian Privacy Commissioner
4. Legal disputes about interpretation of the amendments may constrain the Commissioner’s enforcement activities even further
5. Current provisions which arguably require notification have not been used
6. There is no requirement for notifications to the Commissioner to be published
7. All of the Privacy Act exceptions and carve-outs will apply, limiting the application of the law
8. Lengthy delays in identifying that breaches have occurred make it unlikely there will still be a ‘real risk of serious harm’ when entities are considering notification
9. There is no incentive for entities to notify the Commissioner
10. From a regulatory theory perspective, notice laws have limited operation.

Rather than introducing a heavily qualified law which is unlikely to make any real difference, consideration should be given to more effective ways of regulating the security practices of all Australian organisations.

With the December 2015 release of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 for consultation, in response to recommendations made on the passing of the meta-data retention laws, it seems that mandatory data breach notification may be introduced into Australia at some stage in the next few years. In short, the draft bill imposes an obligation on entities covered by the Privacy Act 1988 (Cth), to notify the Privacy Commissioner and affected individuals where the entity reasonably believes that there is a real risk of serious harm arising from unauthorised access to or disclosure of personal information.

The road to the release of this draft Bill has been long and winding: the Australian Law Reform Commission (ALRC) recommended inclusion of a mandatory data breach notification (MDBN) provision in its comprehensive 2008 review of the Privacy Act 1988 (Cth). Draft legislation based on

---

1 Exposure draft – Privacy Amendment (Notification of Serious Data Breaches) Bill 2015
the ALRC’s recommendations was initially proposed in 2012\(^3\) and then again in 2014\(^4\) but failed to pass. The Australian Government released the current draft in early December 2015, inviting public comment before legislation is introduced in Parliament in 2016.\(^5\) The July election effectively postponed the introduction of the legislation but with both sides of politics supporting some sort of MDBN law, it is reasonable to assume that some form of the law will be introduced in the not too distant future. But what effect is such legislation likely to have? This article proposes that there at least 10 reasons why the introduction of a MDBN law is unlikely to have much effect on either disclosure of potential risks to the personal information of Australians which may have been stolen or accidently disclosed or on the security practices of entities covered by the Privacy Act.

Those reasons are discussed below.

1. Little evidence of change from other jurisdictions

Two main reasons are provided for data breach notification laws in the U.S. First, they provide an incentive for organisations to protect sensitive data, as publicly disclosed security failures may harm their reputation and trigger costly remediation activities. Second, they inform individuals whose records were exposed, allowing them to react quickly to mitigate potential damages and in particular reduce the likelihood of identity theft.\(^6\)

A MDBN law first came into effect the State of California in 2003. Since then, 46 other states in the U.S. passed different forms of MDBN laws. Notwithstanding that the laws have been effect for over 10 years and have widespread application, there has been only limited investigation into the effectiveness of these laws in terms of achieving their stated purposes.\(^7\) Research published in 2008 noted there was little evidence of any link between data security breaches and identity fraud and noted that, in any case, most notices were ignored.\(^8\) Other research which considered the effect of data breach notifications laws between 2002 and 2009 suggests these laws resulted in a 6% decrease in identity fraud.\(^9\) It might be expected that data breaches would decline as organisations covered by the laws improved their security. However, research indicates that the number of data breaches is on the rise,\(^10\) or at the very least remains unchanged.\(^11\)

Anecdotally, one of the main outcomes of the introduction of MDBN laws in the U.S. would seem to be a rise in class action suits against organisations disclosing breaches, a situation not so likely to occur in Australia where the private right to sue for breach of privacy is at best unclear.

---


\(^6\) R.J. Sullivan and L. Maniff, ‘Data Breach Notification Laws’


\(^8\) Cate, F. H. Information Security Breaches: Looking Back and Thinking Ahead (2008)


\(^10\) R.J. Sullivan and L. Maniff, ‘Data Breach Notification Laws’

\(^11\) B. Edwards, S. Hofmyer and S. Forrest, ‘Hype and Heavy Tails: A Closer Look at Data Breaches’ WEIS 2015, <weis2015.econinfosec.org/papers/WEIS_2015_edwards.pdf>. One of the reasons for the number of breaches remaining static is that security has improved at the same rate as attacker prowess (in Conclusion).
2. Inappropriate provisions
Assuming that MDBN laws may have some impact, research indicates that the particular provisions in the proposed Australian law are unlikely to be effective and will have little impact on identity theft.

An investigation into the particular provisions in the different U.S. State MDBN laws identified those more and less likely to result in lower identity theft. Provisions likely to support reduced identity theft include those which indicate active enforcement by the relevant regulator and those which provide incentives to organizations to comply with notification requirements. Provisions that have not been so effective are those giving an organization control regarding notification, such as those requiring notification only if the entity determines there is potential harm to an exposed consumer or if it adopts a relatively weak method of encrypting sensitive data. The proposed Australian legislation has been constructed around the type of provisions identified as being least effective in reducing identity theft. Under the Australian legislation, the entity has responsibility for determining whether there is a breach which carries with it a real risk of serious harm and can take into account considerations such as whether the compromised data would be ‘intelligible’ to an ordinary person (which includes consideration of encryption).

There are no additional rights of action or other enforcement tools provided to the Commissioner in regard to reported data breaches, so little to indicate active enforcement.

3. Resource restrictions will constrain compliance and enforcement activities
The Australian Privacy Commissioner does not have the resources or the powers to conduct deep technical analyses of data breaches to determine key elements such as the cause of the breach, when it occurred, the data compromised and where the data has gone or to advise on whether or not the mitigation activities undertaken or proposed by the breached organisation are appropriate. In most cases the Commissioner will be relying on the information provided by the entity itself based on its own investigation. Historically, the limited resources and capabilities of the Commissioner have had an impact on investigation outcomes.

There is little indication that the Privacy Commissioner will receive significant additional resources or funding to support complex investigations into data breach cases. Similarly, there is little indication of additional resources being available to support the compliance efforts (such as education, guidance and audit) that should be part of any principle based regulatory system. Research

12 Ibid.
13 Ibid.
14 See paragraph 26WB(2)(a) Exposure draft – Privacy Amendment (Notification of Serious Data Breaches) Bill 2015
15 Paragraph 26WB(3), titled ‘Relevant matters.’
16 See for example, the Commissioner’s finding of no failure to comply with the privacy principles in its investigation of Sony reported in Sony Playstation/Qriocity Own Motion Investigation, September 2011 <https://oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity> as compared to the investigation by the UK Information Commissioner’s Office that resulted in findings of failure and a £250,000 fine.
17 The Office of the Australian Information Commission has been allocated $37 million over the next 4 years to support all of its privacy and FOI activities. Budget 2016: Govt finally provides funding for OAIC, Renai LeMay Delimiter, 3 May 2016 <https://delimiter.com.au/2016/05/03/budget-2016-govt-finally-provides-funding-oaic/>.
suggests that periodic audits of security systems can greatly enhance the effectiveness of notification laws.\(^\text{18}\) Since March 2014 the Commissioner has had the power to carry out assessments of whether personal information is being maintained and handled in accordance with the Privacy Principles by all entities covered by the Act (not just public sector entities).\(^\text{19}\) To date, that power has been used sparingly.\(^\text{20}\) It could not be regarded as supporting the sort of periodic audits identified as enhancing the efficacy of MBND laws.

In view of these resource restrictions and limited use of powers to date, regulated entities are unlikely to be overly concerned about active enforcement: active enforcement being one of the indicators of effective MDBN provisions.\(^\text{21}\)

4. Legal Disputes about Interpretation

Lawyers have already indicated they will have a field day with the interpretation of key terms in the proposed legislation such as ‘real risk of serious harm’, with submissions to the Commissioner on the consultation draft legislation referring to the uncertainty in legal understanding of the meaning of these terms and others.\(^\text{22}\) Successive Privacy Commissioner have indicated little interest in having interpretations of the Privacy Principles tested by the courts.\(^\text{23}\) Very few cases have made it to the court system where the Commissioner has tested the meaning of key terms, the current appeal from the AAT finding in the Telstra and Benn Grubb case being one of the first.\(^\text{24}\) Litigation is expensive and it is likely, given the history and the resource constraints impacting the Commissioner, that the Commissioner will be reluctant to take expensive and time consuming legal action against well-funded and litigious entities over the interpretation of the MDBN provisions. Again, this is likely to have an impact on the extent to which the Commissioner may be regarded as likely to actively enforce these provisions, one of the factors important in successful MDBN laws.

5. Little use of existing laws

Many listed organisations are already covered by an obligation to report events that might have a material effect on their share price. s674(2) Corporation Act and ASX Listing Rule 3.1 (which only applies to entities listed on the Australian Securities Exchange) require covered organisations to disclose to the market all information that a reasonable person would expect to have a material


\(^{19}\) Section 33C Privacy Act.

\(^{20}\) Details of assessments by the Commissioner are published on the Commissioners website at <https://oaic.gov.au/privacy-law/assessments/>. Recent assessments include a review of loyalty schemes operated by two major retailers and practices in GP clinics.


\(^{22}\) See, for example, the submission by the Law Council of Australia, published at <https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx>.


effect on the price or value of the entity’s securities if that information was generally known. To date, there has been no notification to the ASX or ASIC of a data breach.

Part of the reason for this may be uncertainty as to whether a data breach would have an effect on the share price if generally known. There has been some research on the impact of security breaches on share price which suggests that there will only be an lasting impact where the entity is a technology company or an organisation, like a bank, which is highly reliant on its technical systems operating with integrity.\textsuperscript{25} This is illustrated by the fact that breaches affecting organisations like Sony and retailers TJMaxx and Target in the U.S. and Telstra in Australia have had little long term effect on the share price while breaches of Choicepoint in the U.S. and DistributeIT in Australia had catastrophic consequences.

In any case, the failure to notify data breaches to date to either the ASX or ASIC suggests that many large listed Australian entities are unlikely to construe such incidents as giving rise to a real risk of serious harm. In fact, the reverse is likely: publication of the breach may itself be regarded as more likely to give rise to harm, certainly to the organisation making the notification decision.

6. There is no requirement for notifications to the Commissioner to be publicised

One of the justifications for passage of the MDBN laws has been that increasing general knowledge about the sorts of data breaches affecting the Australian community. However, the Commissioner has no obligation to publish details of the breaches that are notified to the office. Although it is likely that most notified breaches will become part of the public domain, there is no guarantee of this being the case and no real likelihood of the Commissioner making available sufficient details of the notifications received by the office to support any detailed assessment of the Australian data breach landscape. In any case, details of notifications to the Commissioner would only provide part of the story about data breaches affecting Australian organisations because of the extensive exclusions from the operation of the new MDBN laws.

7. Limited application

Many of the major types of organisations that suffer data breaches are outside the operation of the Privacy Act e.g. local councils, universities and State run health service providers. There has been no suggestion so far that State governments will introduce data breach notification provisions as part of the different State privacy laws. Small businesses,\textsuperscript{26} which are regarded by some as the weakest link in the security eco-system, are also not covered by the data breach notification provisions, being outside the operation of the Privacy Act.

8. Delays in identifying breaches

Most organisations don’t find out that they had a data breach until well after it has occurred. It has been reported that the average time between the occurrence of a data breach and notification to customers is 117 days.\textsuperscript{27} Other research found that the time to identify and time to contain breaches resulting from malicious and criminal attacks was 229 and 82 days respectively. The time for data breaches caused by human error was 162 and 59 days respectively.\textsuperscript{28} External sources, such as law


\textsuperscript{26} Defined in the Privacy Act as those with an annual turnover of $3million or less, subject to ‘carve-ins.’

\textsuperscript{27} Sullivan and Maniff, 69.

\textsuperscript{28} Ponemon Institute, 2016 Cost of data breach study: Global Analysis, 3.
enforcement and third parties, are more likely to detect that an entity has been compromised than the organisation itself becoming aware of the incident through internal controls.\(^{29}\)

Given this time lapse it is probable that any harm likely to result from the breach, such as posting the stolen personal details on underground networks for sale, has already occurred. Notification at this late stage will provide little real opportunity to mitigate any future losses. Any losses will in all probability already have been incurred. This makes the notification of such breaches by the affected entity of little real value.

9. There’s no incentive to report

One of the most common criticisms of MDBN laws is that they provide little incentive for organisations to report data breaches. In fact, some argue that given the cost and exposure involved in data breach notification, there is in fact a dis-incentive. Others suggest that the law favours those with poor security safeguards who are less likely to discover that their systems have been compromised in some way or that there has been any unauthorised access to or loss of data.

Incentives for organisations to comply which could have been considered might include caps on liability or penalties imposed by the Commissioner or protection from civil claims. Inclusion of such incentives may have supported higher reporting numbers.

10. Limited operation from a regulatory theory perspective

A detailed study of the Australian community’s view of MDBN was conducted in 2010. Findings from that research include that data breach notification should be part of a broader set of laws managing information security. In particular, it recommended the introduction of a broader set of laws ‘that focus specifically on the development of legal principles related to corporate information security management.’ Such laws could play an essential regulatory role regarding the protection of personal information and the protection of critical information infrastructures that hold our personal information and are now such an integral part of our information-based societies.\(^{30}\)

To date, notwithstanding that many entities (including AISA) have recommended that consideration be given to introducing a broader range of regulatory measures around security, there is no suggestion that this will be pursued.

Conclusion

There are many reasons (in addition to the 10 listed above) why the introduction of MDBN laws as proposed and in isolation from other regulatory interventions is unlikely to have a significant impact on the Australian data protection landscape. At best, MDBN laws should be regarded as a first step in implementing a more comprehensive approach to ensuring the protection of personal information.

Without the support of a broader framework of regulation, including both incentives and sanctions for entities that take or fail to take appropriate action to secure their systems and sensitive data, it is unlikely that there will be any significant change in the security measures implemented by most Australian organisations to protect information about Australians.

---

\(^{29}\) Verizon 2016 Data Breach Investigations Report, 11.

Dr Jodie Siganto CISSP

Director, IT Security Training Australia

Jodie_siganto@itsecuritytraining.com.au

www.itsecuritytraining.com.au