# THE GOVERNANCE OF THINGS – Mandatory Data Breach Notification

## DÉJÀ VU?

Mandatory data breach notification is almost across the finish line. Or is it?

As many of our readers may know, the third incarnation of a bill that would require all entities bound by the Privacy Act to notify the regulator and consumers of their data breaches was read in parliament in mid-October.

But, with the spring sitting of parliament nearly over, it appears possible that passage will be pushed to 2017, assuming the bill continues to carry enough political force to be passed. After all, the news cycle has moved on from the mandatory data retention reforms which set the context for the Parliamentary Joint Committee on Intelligence and Security's (PJCIS's) recommendation in favour of mandatory breach reporting and the political impetus which followed.

As Peter Leonard previously wrote: "Australian privacy professionals are familiar with notification fatigue. It is the sense of déjà vu we each experience as we turn the pages of yet another call for submissions as to mandatory data breach notification for Australia."

And indeed, we might be fatigued if this bill was to suffer any further setbacks. Its first predecessor, the *Privacy Amendment (Privacy Alerts) Bill 2013,* lapsed when parliament was prorogued before the 2013 election. Its second predecessor was an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*, which was opened for consultation earlier this year. The current bill is a response to the 47 public submissions that were received at that time.

## LEARNING FROM OVERSEAS JURISDICTIONS

Australia is not the first country to consider introducing a mandatory breach notification scheme. The United States has more than 47 states with mandatory reporting in place and 30 of those regimes were in force before 2008 when the Australian Law Reform Commission (ALRC) first proposed mandatory reporting here. Elsewhere, the European Union has introduced regulations that mandate data breach notification. In May 2014, New Zealand announced plans to introduce a two-tier mandatory data breach notification scheme. In June 2015, Canada passed legislation to introduce a national mandatory data breach notification scheme.

And this brings us to the crux of this article. With all of these jurisdictions implementing mandatory reporting regimes before us, what insights have we taken that would support the introduction of the regime or at least the regime in its present form? What do the experiences of others tell us about the appropriateness of the threshold? Are the consumer benefits on which the bill is centred, being delivered, and at what cost? With this bevy of overseas mandatory reporting jurisdictions to observe, one would think the benefits of breach reporting would not only be quantifiable but extrapolated for Australia, too.

The closest we get to reflecting on foreign learnings is a statement in the explanatory memorandum (EM) that the proposed threshold in Australia should follow the ALRC's recommendation for a higher threshold than is provided in "most jurisdictions" to reduce the compliance burden on agencies and organisations.

## CONSUMER BENEFITS

The bill purports to beef up consumer protection. The EM states that mandatory reporting will "allow individuals whose personal information had been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach… by arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts or taking preventative measures, such as changing passwords and cancelling credit cards."

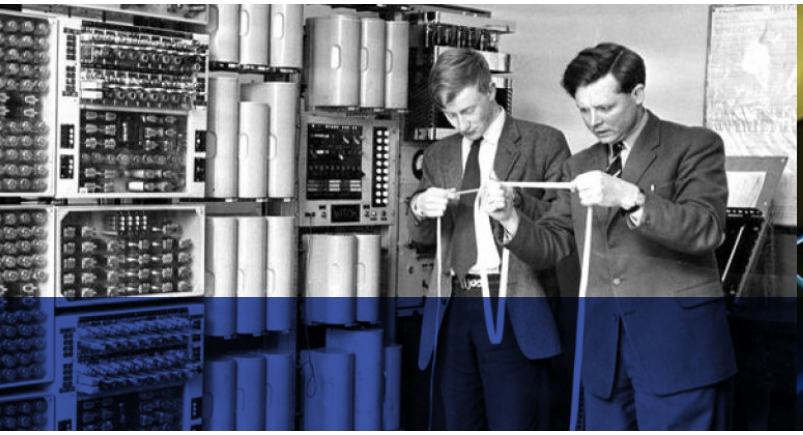
It seems, then, that reporting will bring with it at least two consumer benefits:

- Individuals who are notified might be able to take action to mitigate or minimize the harm (defined as "physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm") that may have otherwise followed were the breach to have occurred without their knowledge;
- With pressure mounting for organisations to be transparent, they will have better regard to data security both to prevent breaches and to have their houses in order, lest the regulator and media come a-knocking. Assuming organisations implement effective compliance regimes, these outcomes will benefit consumers. On this, the threat of a civil penalty of up to 2000 penalty units (or $1.8 million for a corporation) for non-compliance might help privacy practitioners get the attention of management, but in the longer term, we will need to see those fines imposed to keep our boards and funders engaged.

One might wonder whether the bill would materially improve things for consumers of financial services, given banks are already highly motivated notifiers when credit cards or accounts are compromised. The one thing that might change for retail banking customers is that the regime requires the entity to provide a "description of the eligible data breach that [it] has reasonable grounds to believe has happened." Hence, a notice that tells a customer that cards are being replaced, but fails to say why, will no longer make the grade. Somewhere down the line, it is inevitable that we will be asking whether being informed of breaches in all their glory is helpful and brings about a better outcome than simply having the financial risk mitigated through, for example, the issuing of new cards.

## THRESHOLD

The next question is whether the threshold is set appropriately so the objective will be met without "notification fatigue" occurring (that old chestnut). On this, one of the key changes made to the bill following consultation this year is the raising of the reporting threshold. Breaches were previously notifiable if they resulted in a "real risk" of serious harm. They are now notifiable if there is a "likely" risk of serious harm to affected individuals. A real risk was one that was not remote. A likely risk is one that is more probable than not. In other words, less reporting required.



## THE GOLDILOCKS EFFECT

One of the reasons for raising the threshold is to prevent fatigue. Notification fatigue is bad because it can desensitize and make inert those very consumers that need to take preventative measures. While we don't actually know that too much reporting would lead to consumer inertia, data from other jurisdictions might be telling. It could, arguably, lead to fear – paralyzing consumers not from taking steps to minimize the immediate impact of a breach, but from freely participating in the digital economy. Put differently, fear is very bad for trust.

Communicating openly and transparently with consumers is something organisations and government agencies should voluntarily build into their strategies and procedures for managing data breaches. Involving customers in the strategy can, in many instances, enable harm to be reduced and importantly, gives customers some control over a damaging situation in which they would otherwise be disempowered.

Reporting breaches can help protect a brand from damage, which may be costlier than the fines, by influencing the conversation. Reporting breaches can, in fact, build trust by showing that the organisation holds the right values, adequate resourcing for privacy and security and a sound response strategy.

The concern with the mandatory framework is that the settings may result in either under-reporting or over-reporting, while failing to produce better outcomes for consumers and costing Australian businesses hugely in compliance overhead.
It seems we have missed the opportunity to learn from other jurisdictions on how their regimes have delivered value.

**MELANIE MARKS**
Specialist - Privacy compliance, policy and strategy
Marks Consulting Australia

## JOIN INFORMATION GOVERNANCE ANZ

The emerging field of information governance requires the engagement of professionals from multiple disciplines, including cybersecurity, data analytics, data privacy, data governance, eDiscovery, information technology, information management, legal, privacy, records management, and risk and compliance.

**We welcome all new Information Governance ANZ members, supporters and sponsors.**

**Join now at - www.infogovanz.com**