A Mandatory Data Breach Notification Scheme for Australia?

Peter Leonard
Partner

31 March 2016

GILBERT+TOBIN

SYDNEY | MELBOURNE | PERTH

CONTENTS

1 Introduction

The Australian (Federal) Government's consultation paper as to the *Privacy Amendment (Notification of Serious Data Breaches) Bill* 2015 notes the proposed "relatively higher notification threshold" is intended to "help avoid the risk of individuals experiencing 'notification fatigue' and will also help avoid unnecessary administrative costs for business".

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.

But this time it may be different. The current federal Government agreed to introduce a mandatory data breach notification scheme, and to consult on draft legislation, in response to the February 2015 inquiry report1 of the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014.2 Fulfilment of that commitment, rather than consumer expectations or overseas examples of mandatory data breach notification, may well drive the progress of this proposed Bill.

Or it may be the case that our sense of *déjà vu* will be reinforced. The comparable *Privacy Amendment (Privacy Alerts) Bill* 20133 passed through the House of Representatives of the last (43rd) Australian Parliament, but lapsed without Senate consideration when that Parliament was prorogued for the last Federal election. Given progress toward a Federal election this year, this Bill may not proceed past consultation into revision and introduction into the 44th Parliament, or through to passage, before the 44th Parliament is prorogued for the next Federal election.

That would be a great pity, regardless of whether you are, or are not, a proponent of mandatory data notification. Why? Because:

- the draft Bill4, while flawed, is a good basis to work with,
- the consultation5 (which closed on 4 March 2016) on the draft Bill elicited in excess of 40 open submissions6, many of which make thoughtful and sensible suggestions for improvement of the draft Bill,
- some businesses and agencies covered by the federal *Privacy Act* 1988 ("**APP entities**") still don't appear to understand the importance of good information handling and reliable processes and practices of protecting information security, including of consumer privacy. Given limited resources of the Australian Information Commissioner, mandatory data breach notification may be an appropriate discipline upon these less responsible APP entities,
- further delay of any Federal statutory response increases the risk of pre-emptive State or Territory response, perhaps based in frustration at the slow progress of a Federal response and concern that consumer unease about new privacy affecting initiatives, including as to sharing of health related data and through deployment of internet of things (IoT) devices, may delay their uptake. It is in the interest of governments and the business sector to promote consumer

1 Available through http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention.
2 Later the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015 and available at https://www.legislation.gov.au/Details/C2015A00039
3 Available at http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5059.
4 Available at https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx.
5 Australian Attorney-General's Department, Serious data breach notification consultation documents, available at https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx
6 Also available at https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx

confidence in handling of consumer data. Consumer confidence requires openness of APP entities, including when things go wrong,

- a well-considered Federal Bill would be a good precedent for State and Territory based responses covering those entities that are subject only to State based privacy laws, in particular State and Territory government departments, agencies and state owned corporations. That noted, it would be unfortunate if those entities covered by State or Territory and Federal laws, in particular health service providers, were subject to two separate privacy breach notifications schemes each requiring notifications to affected individuals but with differing standards or other requirements.

2 The current position: APP 11 and voluntary data breach notification

The Australian Privacy Principles (**APPs**) in the federal Privacy Act apply to APP entities, being most Australian Government agencies and to private sector organisations with over $3 million in annual turnover (subject to some exceptions for smaller businesses, such as those that are private health service providers, that sell or purchase personal information or that are operating under Australian Government agency contracts).

APP 11 - *security of personal information* requires APP entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP 11 states:

> 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
>
> a. from misuse, interference and loss; and
>
> b. from unauthorised access, modification or disclosure.
>
> 11.2 If:
>
> a. an APP entity holds personal information about an individual; and
>
> b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and
>
> c. the information is not contained in a Commonwealth record; and
>
> d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;
>
> the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

APP 11 has been the subject of useful guidance from the Australian Information Commissioner, most notably:

- OAIC, *APP Guidelines*, Chapter 11: APP 11 — Security of personal information7; and
- OAIC, *Guide to securing personal information*, January 2015.8

The Bill (if enacted) would supplement the operation of APP 11 by amending the federal Privacy Act to introduce a new mandatory data breach notification scheme for certain regulated entities, namely public

7 https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information
8 https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

sector agencies, private sector organisations, credit reporting bodies, credit providers and file number recipients. The Bill would insert a new Part IIIC in the federal Privacy Act, which would:

- cover personal information, credit reporting information, credit eligibility information and tax file number information,
- define when a 'serious data breach' occurs, and
- set out the requirements for when, in what form and to whom, notification of serious data breaches must be given.

The Australian Information Commissioner is already responsible for mandatory data breach notifications under the *My Health Records Act* 2012 (formerly known as the Personally Controlled Electronic Health Records (**PCEHR**) scheme). Given low take-up of that scheme and coverage of mandatory data breach notification being limited to the My Health Records (formerly the PCEHR) System Operator, registered repository operators, and registered portal operators, it is perhaps not surprising that there do not appears to have been any notifications under that Act. However, the OAIC *Guide to mandatory data breach notification in the PCEHR syste*m, September 20159 addresses requirements for compliance with that scheme. That Guide will no doubt be a relevant reference for the Commissioner in developing guidance as to this new Bill if enacted.

The OAIC already receives voluntary data breach notifications. The OAIC received 117 voluntary data breach notifications in the July 2014-June 2015 financial year and 55 voluntary data breach notifications between 1 July and 31 December 2015.10

The Commissioner has issued a Guide as to the Commissioner's expectations as to such notifications: OAIC, *Data breach notification — A guide to handling personal information security breaches*, August 2014.11 That Guide sets out a *Data breach response process* as reproduced overleaf.

The Commissioner's voluntary data breach notification guide is quite detailed and practical and also based upon a threshold of 'real risk of serious harm to an individual'.12 We highlight below just a few features for later comparison to the draft Bill:

- Consideration of **harm assessment** in relation to **access controlled data**. "Is the personal information adequately encrypted, anonymised or otherwise not easily accessible? Is the information rendered unreadable by security measures that protect the stored information? Is the personal information displayed or stored in such a way so that it cannot be used if breached? For example, if a laptop containing adequately encrypted information is stolen, but is subsequently recovered and investigations show that the information was not accessed, copied or otherwise tampered with, notification to affected individuals may not be necessary."
- Review of **when the notification threshold is reached**. "If a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified. However, the challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will

9 https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-dbn-in-pcehr-system
10 Opening statement by Timothy Pilgrim, Acting Australian Information Commissioner, to Senate Estimates Committee on 15 February 20916, available at https://www.oaic.gov.au/media-and-speeches/statements/opening-statement-by-timothy-pilgrim-acting-australian-information-commissioner-to-senate-estimates
11 https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches
12 This test is as recommended by the Australian Law Reform Commission in *For Your Information,: Australian Privacy Law and Practice* (ALRC Report 108) 2008, Chapter 51 (Data Breach Notification)

not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required."

- Discussion of **who should be notified?** "Generally, it should be the individual(s) affected by the breach. However, in some cases it may be appropriate to notify the individual's guardian or authorised representative on their behalf."

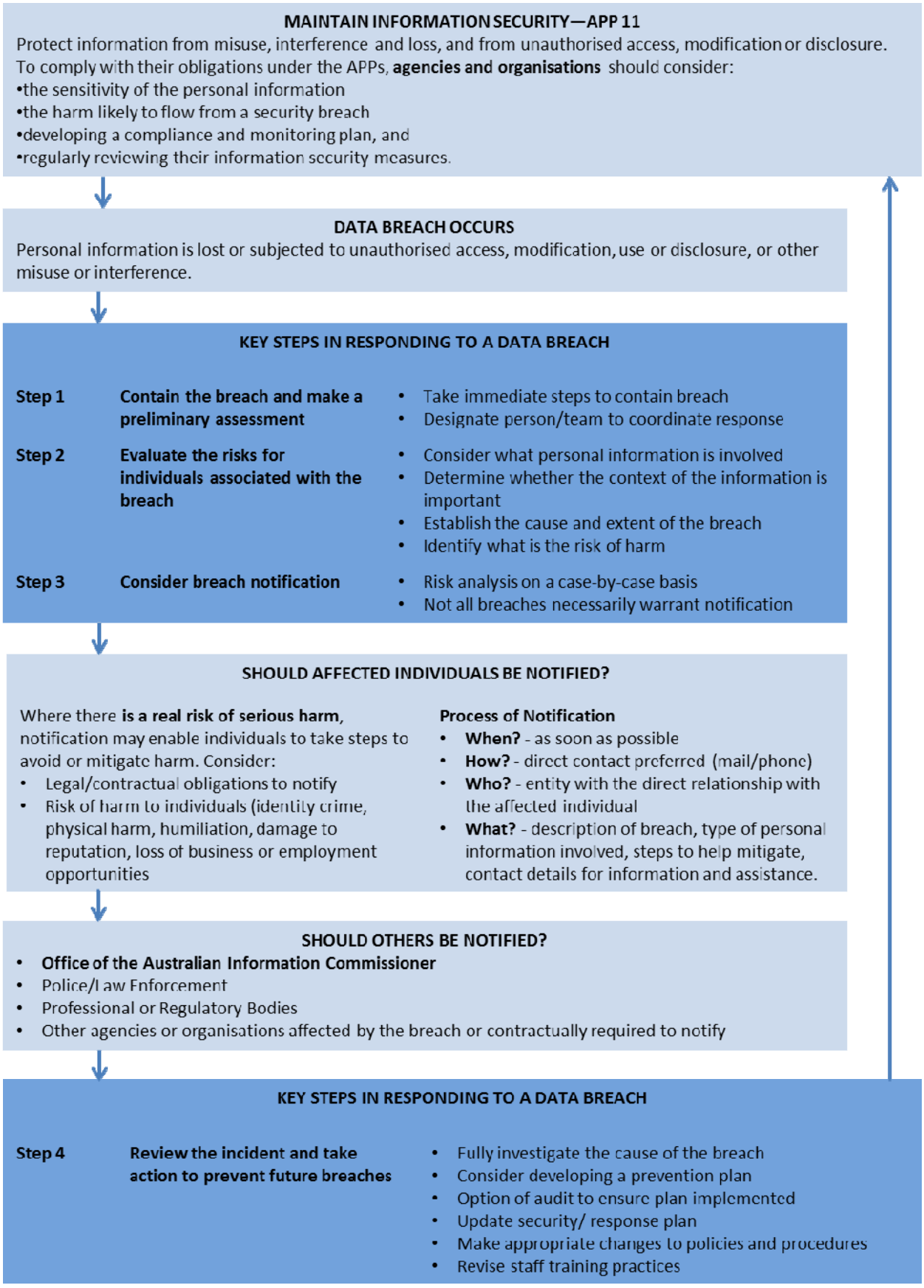
- Review as to **who should notify**. "Typically, the agency or organisation that has a direct relationship with the customer, client or employee should notify the affected individuals. This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate. Joint and third party relationships can raise complex issues. For example, the breach may occur at a retail merchant but involve credit card details from numerous financial institutions, or the card promoter may not be the card issuer (for example, many airlines, department stores and other retailers have credit cards that display their brand, though the cards are issued by a bank or credit card company). Or the breach may involve information held by a third party 'cloud' data storage provider, based outside of Australia. The issues in play in each situation will vary. Organisations and agencies will have to consider what is best on a case by case basis. However some relevant considerations might include:

  - Where did the breach occur?

  - Who does the individual identify as their 'relationship' manager?

  - Does the agency or organisation that suffered the breach have contact details for the affected individuals? Are they able to obtain them easily? Or could they draft and sign off the notification, for the lead organisation to send?"

Data breach response process



3 International standards for data breach notification?

There is no international standard for data breach notification.

In the U.S.A., 'reasonable' security standards are still being debated. Nearly every U.S. state has a different breach notification law, with widely varying notification thresholds. 47 states and the District of Columbia have each passed their own laws that require notifications in certain circumstances. Alabama, New Mexico and South Dakota are the only states without breach notification laws.13

In Canada, the *Digital Privacy Act* of June 201514 amended Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**). While other provisions of the Digital Privacy Act are now in force, those dealing with breach reporting, notification and recordkeeping will come into force after regulations outlining specific requirements are developed and in place.

Canadian organizations will be required report to the Office of the Privacy Commissioner of Canada (**OPC**) and to notify affected individuals and relevant third parties (in certain circumstances) about "breaches of security safeguards" that pose a "real risk of significant harm" to those affected individuals.15 "Breach of security safeguards" is defined in PIPEDA. The concept of "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit report and damage to or loss or property.16 Factors that organizations need to consider when assessing presence of a real risk of significant harm include the sensitivity of the information involved and probability that the information was or will be misused.

Notification to affected individuals and reporting to the OPC will be required as soon as feasible after an organization determines that the breach has occurred. An organization will also be required to notify any other organization or government institution if it believes the other body may be able to reduce the risk of or mitigate the harm. For example, a retailer could notify a credit card issuing bank or law enforcement agency. The consent of individuals would not be required for such disclosures.

Organizations will also be required to keep a record of all breaches involving personal information and provide a copy to the OPC upon request. Organizations that knowingly fail to report to the OPC or notify affected individuals of a breach that poses a real risk of significant harm, or knowingly fail to maintain a record of all breaches, could face fines of up to CAN$100,000.

In Europe, *Data Protection Directive 95/46/EC* is silent as to data breach notification to affected individuals. However, under Article 4 of *Electronic Communications Directive 2002/58/EC*, providers of publicly available electronic communications services are obliged to notify the competent national authorities, and in certain cases also the subscribers and individuals concerned, as to personal data breaches.17 The Article 29 Data Protection Working Party has provided relevant guidance18 as to the expectations of national supervisory

13 See for example National Conference of State Legislatures, *Security Breach Notification Laws*, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx and for a useful summary BakerHostetler *Data Breach Charts*, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf. See further Jeffrey Kosseff, *My company has had a breach: Whom do I have to notify?* iapp *Privacy Advisor*, 21 March 2016 available through https://iapp.org/news/

14 Available through https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.asp

15 Sections 10.1(a) and (c)

16 Section 10.1(7)

17 See further Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

18 Opinion 03/2014 on Personal Data Breach Notification adopted 25 March 2014, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf. See also the useful materials

authorities in the 28 EU member nations. Each nation variously states requirements and expectations as to notification of data breaches as variously defined.

The new *General Data Protection Regulation* (**GDPR***)* is intended to bring new harmonisation. The draft was finally generally agreed upon by the European Parliament and Council in December 201519 and would become law if formally adopted by the European Parliament and Council.

Under the GDPR, a "personal data breach" is notifiable20 to the relevant data protection authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it". If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. A "personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". Unlike many U.S. state data breach laws, the GDPR does not state a trigger for notification to the data protection authority of likelihood or possibility of fraud or identity theft or other significant adverse consequence for affected individuals. However, proposed Article 31(1) contains an exception to the general requirement for notification to the data protection authority of "personal data breach": notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals". It is difficult to see how this exception can be given practical effect, given the vagueness of the language and the potential jeopardy if an entity gets it wrong. The GDPR includes large fines: up to 1,000,000 Euros or, in the case of an enterprise, up to two percent of its annual worldwide turnover.

The GDPR provides that when a data processor experiences a personal data breach, it must notify the data controller. A data processor otherwise does not have relevant notification or reporting obligations under the GDPR.

If a data controller determines that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals", the data controller must also communicate information regarding the personal data breach to affected data subjects. Under Article 32, this must be done "without undue delay". The GDPR provides exceptions to this additional requirement to notify affected data subjects in the following circumstances:

- the controller has "implemented appropriate technical and organizational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption";
- the controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialize; or
- when notification to each data subject would "involve disproportionate effort", in which case alternative communication measures may be used.

The relevant data protection authority may require notification, or conversely, determine (in effect, confirm) that it is unnecessary under the circumstances.

---

available at European Union Agency for Network and Information Security, Data breach notifications https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn.

19 The final drafts out of the so-called 'trilogues' are most conveniently available through the iapp global website at https://iapp.org/resources/topics/eu-data-protection-reform/.

20 A notification to the authority must "at least": (1) describe the nature of the personal data breach, including the number and categories of data subjects and data records affected; (2) provide the data protection officer's contact information; (3) "describe the likely consequences of the personal data breach"; and (4) describe how the controller proposes to address the breach, including any mitigation efforts. If not all information is available at once, it may be provided in phases.

4 The draft Bill – key features and some associated concerns

Key features of the draft Bill include:

4.1 **Notification through a section 26WC(3) statement** would be required to be given to the Commissioner and to all individuals in relation to whom relevant information was held where "there are reasonable grounds to believe" that information was the subject of a "serious data breach".

4.2 **A serious data breach** would occur if unauthorised access to, or unauthorised disclosure of, any of personal information, credit reporting information, credit eligibility information, tax file number information "will result in a real risk of serious harm to any of the individuals to whom the information relates"21, or any of that information is of a kind specified in the regulations.22

The draft Explanatory Memorandum informs us that the second limb (*information of a kind specified in the regulations*) is "intended to provide the flexibility to deal with data breaches where loss of particularly sensitive information may result in unauthorised access or unauthorised disclosure. Paragraph 26WB(2)(c) would apply regardless of the likelihood of such access or disclosure actually occurring following the loss, and regardless of the risk of harm that would occur as a result. This again recognises that particularly sensitive information should be subject to the highest level of privacy protection."23

However, the Bill allows for regulations to significantly expand the definition of serious data breach beyond the first limb: note that the second limb is not limited to sensitive information and could potentially apply to any of the information referred to in section 26WB(1).

4.3 A risk of harm is real if it is "not remote".24

Harm is defined inclusively, not exhaustively, and includes all imaginable harms - physical harm, psychological harm, emotional harm, harm to reputation, economic harm and financial harm.25

Given that the notification requirement arises under paragraph 26WC(1)(c) in relation to "*each of the* individuals to whom the relevant information relates" wherever the loss or unauthorised access or disclosure will result in a real risk of serious harm to "*any of the* individuals to whom the information relates"26, a not remote risk of harm (as so broadly defined) may frequently arise. That is, the notification requirement does not appear to be limited to individuals whose information was compromised: notification appears to be required to all individuals in relation to whom information of the nature compromised is held, whether or not compromised in relation to some (or most) of those individuals. Having regard to both the underlying principles and the overseas precedents this is unusual, but the Explanatory Memorandum makes it clear that the drafting is deliberate:

> 78. The requirement to take such steps (if any) to notify affected individuals will apply even in cases where information about multiple individuals is compromised in a serious data breach, but only some of those individuals are at real risk of serious harm as a result. This recognises that, particularly where a serious data breach involves a large number of individuals, it may require an unreasonable volume of resources for an entity to assess which affected individuals are at real risk of serious harm and which are not. Notification to the entire 'cohort' of affected

21 Draft section 26WB(2)(a)(i)
22 Draft section 26WB(2)(a)(ii)
23 Draft Explanatory Memorandum para 32
24 Draft section 26WG
25 Draft section 26WF
26 Draft section 26WB(2)(a)(i)

individuals may actually reduce the cost of compliance for entities, and would also allow each individual to consider whether they need to take any action in response to the serious data breach.

79. An example of how paragraph 26WC(1)(c) could apply would be a serious data breach involving unauthorised access to an entity's customer database which contained the credit card details of some individuals but not others, where the real risk of serious harm arising from the data breach involves potential credit card fraud that could only apply to the former group. Following notification, individuals in the former group could consider cancelling their credit card or alerting their financial institution to the potential risk of fraud, while individuals in the latter group could consider whether they are at real risk of serious harm. If notifying each affected individual under paragraph 26WC(1)(c) is not practicable, the entity could consider whether the alternate notification arrangements in paragraph 26WC(1)(d) below are available.

However, this reasoning appears contrary to avoiding "risk of 'notification fatigue" among individuals receiving a large number of notifications in relation to non-serious breaches".27 In the situation now under consideration, may individuals may receive notice in relation to a breach which is not serious in relation to them, thereby creating both potential for immediate and unnecessary anxiety and subsequent notification fatigue.

Query why in this situation an APP entity should not be free to determine in relation to which individuals the breach is serious and then to provide notice to those individuals only. The Bill could readily provide that APP entity risks contravention if that selection is not reasonable, or alternatively require the APP entity to explain the basis for its selection as to 'affected individuals' to the Commissioner. The OAIC submission makes it clear that the Commissioner sees it as sensible for APP entities to be able to make their own assessment of whether a breach is sufficiently serious to warrant notification and then to determine which individuals are affected and should be notified, without regulatory jeopardy provided that the entity has taken reasonable steps to assess the breach and is satisfied that the breach is not serious.28 It is suggested that the Commissioner's reading is to be preferred to the current drafting and should be given effect in any revision of the draft Bill.

4.4 A related question is **whether the same statement as to a serious breach should go to the Privacy Commissioner and affected individuals**, or whether a two-step process is more appropriate. The Business Software Alliance submission relevantly notes:

> BSA would encourage the Australian government to follow best practices that exist in other regions and should not create a new regime that is out of step with international systems. For instance, one emerging best practice is a two-step approach for breach notification:
>
> a. Under these regimes, the controller should without undue delay after having become aware of the breach notify the personal data breach to the competent supervisory authority, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.
> b. The individuals are solely notified if the personal data breach is likely to result in a significant risk of harm to individuals, in order to allow them to take the necessary precautions. The communication to the data subject is not be required if:

27 "Notification fatigue' is referred to in the Explanatory Memorandum General Outline at para 8 and again in the notes on clauses at paragraphs 7, 33, 87, 111 and 129. Oddly, this concern is not expressed in relation to the expansive notification requirement in paragraph 26WC(1)(c).
28 https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx at pages 5-6

i. appropriate technical and organisational protection measures were implemented and applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

ii. subsequent measures to ensure that the significant risk of harm to data subjects is no longer likely to materialize have been taken by the controller; or

iii. it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.29

4.5 When is there a risk of "serious" harm?

Neither the draft Bill nor the Explanatory Memorandum provide any guidance. The list of "relevant matters" in section 26WB(3) is useful as to real risk of harm, but not useful as a gauge to 'seriousness'. We are told that "The risk of harm must be real, that is, not remote, for it to give rise to a serious data breach"30, but this just introduces circularity as to "real risk" and "serious harm". Given that harm can be psychological or emotional harm to any affected individual, and other Australian law as to 'serious harm" is highly specific to its statutory context and therefore not a useful guide, it is likely that "serious" does not add much to "real". Looking all the way back to the ALRC Report, we are told that "In international law, the term 'a real risk of serious harm' has been defined to mean 'a reasonable degree of likelihood', 'real and substantial danger' and 'real and substantial risk'.31 So "serious" appears to mean something more than trivial or insubstantial, but just how much more is indeterminate. A state of distress or anxiety is not necessarily "harm", but again the boundary is unclear: there is no clear measure of seriousness in the absence of any objective measure, such as a person of ordinary sensibilities and not extraordinary sensitivity.

It is noted that the Commissioner is empowered and expected to issue guidance. However, it is difficult to see what guidance the Commissioner could give in relation to "real risk of serious harm" in the absence of clearer direction from the legislature: it is asking the Commissioner to deploy a 'micrometer in a mudpool'. Interesting, ENISA in a working document'32 has endeavoured to build just such a micrometer, scoring severity of a data breach by applying a numerical methodology. Although the methodology may be criticised, at least it attempts to provide organisations assessing where to notify with an objective measure that among other things, distinguishes 'significant inconvenience' from 'significant consequences'. ENISA's work warrants further consideration.

The submission of the Law Council of Australia33 is pertinent:

> 37. The Law Council is concerned by the selection of what might be seen as an inherently subjective test as a matter that is essential to the identification of a 'serious data breach', particularly as clause 26WB(2) primarily requires the consideration of matters going to the seriousness of harm rather than the level of confidence that any harm would be likely to actually occur.
>
> 38. In particular it is far from clear how a possibility objectively assessed as 1 in 100, or 1 in 50, should be assessed under the proposed 'not remote' test. To express this another way, would a

29 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/BSA-Software-Alliance.PDF
30 Explanatory Memorandum, General Outline para 8.
31 Australian Law Reform Commission in For Your Information,: Australian Privacy Law and Practice (ALRC Report 108) 2008, at para [51.85], citing R v Secretary of State for the Home Department, Ex Parte Sivakumaran [1988] AC 958
32 European Union Agency for Network and Information Security, *Recommendations for a methodology of the assessment of severity of personal data breaches*, 20 December 2013, available through https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity
33 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Law-Council-of-Australia.PDF

risk assessed as 'highly unlikely' be assessed as 'remote' or 'not remote'? The Law Council is unable to judge this, and submits that affected organisations also will be unable to do so. For completeness, the Law Council also notes that in a number of risk related fields, attempts have been made to quantify risk descriptions and provide for an element of consistency.

[The submission then cites the following qualitative descriptors:

Probability range	Descriptive term
< 1%	Extremely unlikely
1–10%	Very unlikely
10–33%	Unlikely
33–66%	Medium likelihood
66–90%	Likely
90–99%	Very likely
> 99%	Virtually certain.]34

Serious consideration should be given to streamlining description of data breach related risks and likely impacts.

Recommendation: Replace the 'not a remote risk' double negative test with a positive test, such as 'real risk', 'likely risk' or 'probable risk'.

4.6 Exemptions

Although the Commissioner may exempt an entity from the requirement to provide a notification statement under section 26WC(1), the Commissioner may only do so whether determined to be "in the public interest to do so".35

The Explanatory Memorandum makes it clear that this is intended to address matters of state ("where there is a law enforcement investigation being undertaken into a data breach and notification would impede that investigation, or where the information concerned matters of national security"), not cases where the Commissioner considers that notification is not appropriate.

It would seem sensible to confer a broader discretion on the Commissioner.

34 From Anthony G. Patt and Daniel P. Schrag, 'Using Specific Language to Describe Risk and Probability', *Climatic Change* 61: 17–30, 2003. Klewer, The Netherlands.
35 Draft section 26WC(6).

4.7 An entity must not apply to the Commissioner for an exemption from the notification requirement under section 26WC(1) "that relates to particular circumstances unless the entity believes, on reasonable grounds, that there has been a serious data breach of the entity that involves those circumstances".

This provision, section 26WC(9), is clearly intended to protect the Commissioner from we might call chronic (exemption notice request) fatigue syndrome. However, the wording of this provision is quite problematic. It is not at all clear that the Commissioner may entertain an application for a qualified exemption because, by definition, any exemption could only be granted that relates to particular circumstances that constitute a serious data breach, not those circumstances that relate to individuals in respect of which the breach is not serious.

Again, it would seem sensible to confer a broader discretion on the Commissioner. Chronic applicants for exceptions from the Office of the Commissioner might reasonably expect the same sceptical reception and 'naming and shaming' that awaits habitual APP miscreants today.

4.8 Admissions

Another relevant issue is whether there is a significant disincentive to fulsome breach statement arising from by potential class actions and the fact that breach notifications can appear to be admissions of liability.

Given the that objective of the scheme is to promote transparency through fulsome notification and associated risk mitigation steps, it would be appropriate to provide a safe harbour from subsequent litigation for material included in a section 26WC(3) breach statement and associated material as provided to the OAIC.

5 Other concerns

As noted earlier in this paper, the consultation on the draft Bill elicited in excess of 40 open submissions. Many of these make thoughtful, sensible and detailed suggestions for improvement of the draft Bill. Some of these concerns reflect matters already discussed above. Many suggestions are as to important matters of detail which, although important, are outside the ambit of this paper.

A few further matters are discussed below.

5.1 Multiple notifications and data controllers

The Business Software Alliance36 notes that unlike the EU and some other jurisdictions, the federal Privacy Act does not distinguish between contractors (i.e. data processors) and principals (i.e. data controllers). Proposed section 26WC(1) requires the entity to which the serious data breach has occurred to issue the notices. However, with the increasing growth of the cloud IT services market, in many cases the entity that is holding or processing the relevant information is a contractor of the principal entity that has the relationship with, and collected the personal information from, the individuals to whom the relevant information relates. Indeed, in many cases the contractor may not know the individuals to whom the information relates, as they merely passively hold or process that information on behalf of the principal.

The BSA, Communications Alliance37 and some other submitters suggest that it is more appropriate and efficient for the principal to be responsible for issuing the notice to the affected individuals, rather than the contractor. The obligation of a contractor should be to notify its principals when a serious data breach occurs in respect of the contractor, and the obligation of the principal should be to then provide the relevant notices to individuals that are affected.

For example, Article 4 of the GDPR defines 'data controllers' as the body "which alone or jointly with others determines the purposes, conditions and means of the processing of personal data". The 'processor' is the body "which processes personal data on behalf of the controller". The GDPR establishes a chain of notification: where a notifiable data breach has occurred, Article 31.2 of the GDPR requires that 'processors' alert 'controllers' of such breach, but not more. 'Controllers' are obliged to notify the relevant authorities and affected individuals about a breach. Similarly, many US state data breach notification laws delineate between companies that own or license data and those entities that maintain information on behalf of these data owners. In these cases the data owner must notify affected individuals and state agencies while third parties must notify the data owner. Data owners can contractually require third parties to notify affected individuals.

5.2 "Ought reasonably be aware"

Many submissions pointed to the problem with the obligation to notify attaching to the phrase "ought reasonably be aware" in section 26WC(1). If an APP entity is not actually aware, how can it fulfil an obligation to notify? If an APP entity has breached APP 11.1 by failing to implement systems and protocols that notify the entity of actual or potential data breaches, and because of this the entity fails to notify the affected individuals, there is an "interference with the privacy of an individual" under APP 11.1, and there appears limited utility in imposing liability for a second "interference with the privacy of an individual" arising out of the same underlying conduct and a failure to notify a matter which an APP entity does not in fact know.

36 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/BSA-Software-Alliance.PDF, at pages 2-3
37 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Communications-Alliance.PDF, at pages 3-4

The Australian Broadcasting Corporation noted that having regard to the current threat landscape, the practical reality of sophisticated cyber-attacks is that an entity may not become aware of a serious data breach until after the hacked information has been unlawfully used or disclosed. This may be a significant time after the serious data breach occurred. The ABC cited a study from the cybersecurity firm FireEye finding that organisations take, on average, 229 days to detect a data breach and two-thirds of organisations are informed about the breach by a third party. In those circumstances, the ABC suggested that it will be difficult to determine the point at which the entity 'ought reasonably to be aware' of the serious data breach.38

As a related point, the ABC noted that as presently drafted, proposed section 26WB(5) imposes an absolute obligation on an entity to issue a breach statement in accordance with proposed s.26WC(3) in the event of a serious data breach of personal information held by an overseas recipient (by virtue of APP 8.1). This obligation exists regardless of whether an entity is made aware of a serious data breach by the overseas recipient. It is feasible that an entity may take reasonable steps to ensure that an overseas recipient is required to notify the entity of a serious data breach (for instance, by imposing contractual obligations to that effect), but may nevertheless be unaware of a serious data breach by the overseas recipient (for instance, if the overseas recipient fails to comply with the contractual obligation). In those circumstances, the entity will be unable to comply with proposed section 26WC(3) despite having taken reasonable steps to do so. This is inconsistent with the approach taken to the management of cross-border disclosure of personal information in APP 8.1 which requires an APP entity to 'take such steps as are reasonable in the circumstances'. The ABC submits that further consideration should be given to addressing this inconsistency – or that the requirement to issue a statement under proposed section 26WC(3) of the draft Bill is only triggered when an entity becomes aware of a serious data breach, not from when an entity 'ought reasonably to be aware' that a serious data breach has occurred.

5.3 Loss of encrypted information

A relevant factor in assessing whether there has been a serious data breach is, if the information is not in a form that is intelligible to an ordinary person, "the likelihood that the information could be converted into such a form".39 Some submissions referred to the difficulties in applying the provisions potentially relating to loss or unauthorised access to or unauthorised disclosure of encrypted information.

The Australian Retail Credit Association (ARCA) noted:40

> The concept of safe harbour for encrypted data has formed part of the overseas data breach regimes. In particular, encrypted data has been exempt from California's notification scheme since its inception in 2003 [CA Civil Code, ss 1798.82]. The first significant change to that arrangement occurred in January 2016 when amendments to the Californian scheme commenced. These amendments re-defined "encrypted" to where it is "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."
>
> The Australian Law Reform Commission (ALRC) in its review of Australian Privacy Law, considered the Californian exception for encrypted data, and recommended:

38 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Australian-Broadcasting-Corporation.PDF. See also the Australian Finance Conference submission at pages 4 to 7, as available at https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Australian-Finance-Conference.PDF

39 Draft section 26WB(3)(d). Unfortunately various word formulations are used that make interpretation of section 26WB(3)(d) problematic – in the section itself, "the likelihood" (unquantified) and in para 30 of the Explanatory Memorandum, that loss of information is not a serious breach "if it is not probable" that information will then become subject to unauthorised access or disclosure, but then later in that paragraph, "where the probability of encryption being circumvented is low". These different formulations cannot be sensibly reconciled.

40 https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Australian-Retail-Credit-Association.PDF

> "the provisions should state that, in determining whether there is a real risk of serious harm, consideration should be given to whether the specified personal information was encrypted adequately. The requirement that encryption be 'adequate' implicitly requires that the encryption key was not also acquired by the unauthorised person. In other words, encryption will not be adequate where there is an easy means of decoding the information. This phrasing also avoids any need to specify exactly what type of encryption is adequate. An assessment of adequacy will depend on the circumstances of the case, taking into account matters such as the type of personal information, the nature of the agency or organisation holding it, and the risk of harm that would be caused by its unauthorised acquisition. The Privacy Commissioner should issue guidance on the type and standard of encryption he or she generally will consider adequate."41

As the Communications Alliance noted:

> The GDPR takes a more pragmatic approach by exempting the entity from notifying the affected individual if it "has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption". This approach allows entities to make a much more straight forward assessment of whether there is a 'real risk of serious harm' and it is recommended for adoption in the Australian context.42

41 The Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108), 2008, at 51.92
42 At page 7, available at https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Communications-Alliance.PDF

6 Conclusion

The Federal Government is to be commended for releasing this draft Exposure Bill. The consultation has been refreshingly short on polemics and conducted within a reasonable timeframe. That we have a consultation at all, and can engage in a consultation without polemics, is a very significant improvement upon the processes that recently accompanied, in particular, mandatory data retention for telecommunications service providers and other national security related legislation.

It is important that this consultation results in improvements to the Bill through hard-coded provisions rather than open ended regulation making powers, embellishments in the Explanatory Memorandum, or references to the OAIC issuing guidance. The OAIC is not possessed of greater insight or ability to discern what is a "real risk of serious harm" to affected individuals than this the legislature. Nor should industry be placed in a position of trying to discern perceived psychological or emotional harm that some individuals might suffer without any objective measure of reasonable sensibilities.

The task for legislation like this is not easy. The temptation for the legislature to 'pass the parcel' to the Commissioner, or to industry, is very real. Good law takes good consultation and time. Proponents of mandatory data notification have the ability to achieve good law by revising this Bill.

Peter Leonard

Partner, Gilbert + Tobin Lawyers
T +61 2 9263 4003
pleonard@gtlaw.com.au

31 March 2016


GILBERT+TOBIN
SYDNEY | MELBOURNE | PERTH