Australian Government
Office of the Australian Information Commissioner

Our reference: 15/000172

Commercial and Administrative Law Branch
Attorney-General's Department
4 National Circuit
Barton ACT 2600

By email: privacy.consultation@ag.gov.au

Submission - Mandatory data breach notification discussion paper

I welcome the opportunity to make a submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper) and related exposure draft *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (the Bill).[1]

I also thank the Department for consulting my office (the Office of the Australian Information Commissioner (OAIC)) during the drafting of the Bill.

In this submission I set out:

- the background to the scheme proposed under the Bill
- reasons I continue to support the introduction of a mandatory serious data breach reporting scheme
- anticipated benefits of a mandatory serious data breach reporting scheme
- support for specific elements of the scheme proposed in the Bill, and
- a commitment to assist industry with implementing the requirements of the Bill, including through education and guidance.

Background to proposed scheme

In 2008, the Australian Law Reform Commission (ALRC) recommended that the *Privacy Act 1998* (Cth) (Privacy Act) be amended to impose a requirement on entities to notify the Privacy Commissioner and affected individuals of a data breach that would create 'a real risk of serious harm'.[2]

In February 2015, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) also recommended that a mandatory data breach notification scheme be enacted in the Privacy Act, following its inquiry into new mandatory data retention laws.[3] These laws have now been

[1] www.ag.gov.au/consultations/pages/serious-data-breach-notification.apsx.
[2] *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108), Recommendation 51-1.
[3] PJCIS *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*,

enacted and require telecommunications service providers to collect and retain certain types of data for at least two years.[4]

Support for a mandatory data breach notification scheme

I continue to support the introduction of a mandatory data breach reporting scheme for serious data breaches.[5]

The OAIC continues to see evidence of a high number of serious data breaches. McAfee Labs Threat Report for August 2015, which reviewed changes in cyber threats and cybersecurity from 2010 to 2015, states that there has been a 'monumental increase in the number of major data breaches and in the volume of records stolen'.

Without mandatory reporting of serious data breaches, some entities may not notify individuals that may be affected, or the OAIC.

I believe that a mandatory notification scheme is necessary to:

- give confidence to all Australians that if they are affected by serious data breach, they will be given a chance to protect their interests, and
- signal to entities that protection of individuals' personal information should be a priority in the digital age.

When individuals are told about a serious data breach in relation to their personal information, they are able to take steps to minimise the impact of the breach, such as:

- cancelling credit cards
- changing online passwords, and
- monitoring their credit reports.

Where an entity notifies the OAIC about a serious data breach, the OAIC can:

- give the entity guidance on responding to the data breach
- assist the entity to determine whether the breach has been contained
- meaningfully respond to community enquiries about the breach, and
- explain to individuals steps they may take to protect their personal information.

---

http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/ Report, recommendation 38.

[4] See *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, which amends the *Telecommunications (Interception and Access) Act 1979* (Cth).

[5] See previous OAIC public submissions including to the AGD, on its discussion paper *Australian Privacy Breach Notification*, December 2012, and to the Senate Legal and Constitutional Affairs Committee, on its inquiry into the *Privacy Amendment (Privacy Alerts) Bill 2013*, June 2013 (https://www.oaic.gov.au/engage-with-us/submissions/).

Benefits of the proposed mandatory notification scheme for serious data breaches

Entities will have greater clarity about which breaches need to be reported

Notification is not always an appropriate response to a breach, and a key challenge for entities is to determine if and when to notify individuals and/or the OAIC.[6]

I suspect that many Australian entities do not voluntarily report all serious data breaches or recognise which incidents they should report. Data breaches regularly come to my attention through the media and allegations from third parties.

Following release of the Discussion Paper, IT security firm Threat Intelligence also said that the majority of companies they audited have had customer data stolen, but few reported breaches to the OAIC or affected individuals.[7]

The proposed mandatory notification scheme will:

- clarify for entities what sort of data breach is a 'notifiable breach', and
- help entities assess whether they have experienced a 'notifiable breach'.

There will be consistent reporting between entities

Under the current voluntary or self-regulatory model, entities that tell their customers about a serious data breach may suffer disproportionate reputational damage compared with entities that deal with serious breaches internally.[8]

For example, in 2015, a security vulnerability on a relatively widely used software platform resulted in the exposure of several Australian entities' customer records. Some entities notified affected customers and the OAIC, and experienced adverse media coverage.

I anticipate that as the platform was widely used, other entities may have also experienced a breach but did not notify affected individuals or the OAIC, thereby avoiding media scrutiny.

A mandatory scheme that imposes uniform obligations will place all entities in this type of scenario on a level playing field. In other words, if the breach is a 'notifiable breach', any entity that experiences it will need to notify.

I consider that this will ensure that:

- entities that currently adopt good practises of notifying are not unfairly disadvantaged, and

---

[6] See, for example, the discussion in OAIC's *Data breach notification - A guide to handling personal information security breaches* https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches#scope-of-this-guide.
[7] See Sydney Morning Herald, '*Delayed Australian data breach notification bill lands*', http://www.smh.com.au/it-pro/security-it/delayed-australian-data-breach-notification-bill-lands-20151203.
[8] Jane Winn, 'Are Better Security Breach Notification Laws Possible' (2009) 24 *Berkeley Technology Law Journal* 1133, 1165.

- consumers are provided with more comprehensive and consistent information about data breaches that may affect them.

Notification can help affected individuals mitigate the risks

Data theft and fraud continues to be a concern for Australians. In January 2016, the Australian Cybercrime Online Reporting Network (ACORN) stated that it received 39,000 reports of cybercrime in 2015,[9] and half related to online fraud and scams.

Where personal information has been compromised, notification can be essential to help affected individuals mitigate potential harm.

For example, where an individual's identity details have been stolen, once notified, the individual can take steps to regain control of their information. This may involve cancelling credit cards, changing passwords or requesting new identifiers.

Taking these steps may limit the risks that result when personal information is compromised.

Mandatory notification may assist entities with their response to serious data breaches

There may be benefits for entities that notify affected individuals that a serious data breach has occurred. Proactive and timely notification of a serious data breach:

- allows the entity, rather than the media, to state what has happened and how the entity is managing the breach
- helps the entity rebuild public trust
- demonstrates publicly that the entity takes privacy seriously, and
- demonstrates that the entity is working to protect affected individuals from the harm that could result from the data breach.

There is also evidence that the cost of notification is a relatively small component of the total cost of a data breach. Ponemon Institute's 2015 *Cost of a Data Breach Report* (Ponemon Report)[10] identified that of four key cost components of a data breach, notification related activities represented the lowest cost component.[11]

[9] https://www.ministerjustice.gov.au/Mediareleases/Pages/2016/FirstQuarter/18-January-2016-Australian-Cybercrime-Online-Reporting-Network-receives-more-than-39000-reports.aspx.
[10] Ponemon Institute, *Cost of a Data Breach Report 2015*, http://www-03.ibm.com/security/data-breach/.
[11] Ponemon Institute, *Cost of a Data Breach Report 2015*, http://www-03.ibm.com/security/data-breach/, page 17. The four components were: notification, detection and escalation, ex-post response, and lost business.

The OAIC supports the elements of the proposed scheme

The proposed scheme would require all entities covered by the Privacy Act to notify the Australian Information Commissioner (the Commissioner) and affected individuals of a serious data breach relating to:

- personal information
- credit reporting information
- credit eligibility information, and
- tax file number information.

I believe the proposed scheme will achieve the right balance between empowering individuals to protect their privacy and placing reasonable regulatory requirements on regulated entities.

Only 'serious data breaches' must be reported

A frequent criticism of mandatory notification schemes is that requiring entities to notify every data breach will:

- result in too many notifications, and
- lead to notification fatigue among members of the public.[12]

In other words, if individuals are notified of every minor data breach, individuals may ignore notifications about more serious incidents. This could undermine the effectiveness of a mandatory reporting scheme.

Under the Bill, a data breach is only serious and notifiable when affected individuals face a 'real risk of serious harm' (see s 26WB(2)). I therefore support the proposed scheme that limits the obligation to notify to serious data breaches as this will prevent notification fatigue.

Only requiring entities to notify the OAIC of serious data breaches will also ensure that we are able to focus our resources on breaches that present the greatest privacy risks and, importantly, ensure that the risk to affected individuals is managed.

Entities make their own assessment of whether a data breach is 'serious'

I recognise that a key challenge for entities in responding to a data breach is determining whether the breach is serious, and if and when notification is required.

However, s 26WC of the Bill gives entities the autonomy to make their own reasonable assessment of whether a data breach is serious.

Under this mechanism, an entity can be confident that it will not be liable for a failure to notify the OAIC and affected individuals of a data breach, provided the entity:

---

[12] See for example, Paul Schwartz and Edward Janger, 'Notification of Data Security Breaches' (2006) 105 *Michigan Law Review* 913, 916.

- has taken reasonable steps to assess the breach, and
- is satisfied that the breach is not serious.

This mechanism will enable entities to handle non-serious data breaches under their own privacy procedures, and without fear of liability under the new notification provisions.

The Bill lists considerations to help entities assess whether a data breach is 'serious'

Section 26WB(3) of the Bill lists relevant matters that entities may consider when determining whether a data breach is serious (or whether there is a 'real risk of serious harm').

If an entity conducts an assessment of relevant matters and does not form a reasonable belief that there has been a serious data breach, notification will not be required.

For example, if compromised data is adequately encrypted, given the nature of the data and circumstances of the breach, this will be a factor that weighs against the risk of harm being 'serious'. Depending on other circumstances of the breach, notification may not be needed.[13]

The OAIC considers that this section will give entities more certainty about when the obligation to notify applies.

As the list of relevant matters is non-exhaustive, this section also allows entities flexibility to assess the seriousness of each data breach on a case by case basis.

Entities do not need to notify while making a reasonable assessment

The Ponemon Report suggests that rushing to notify increases the overall cost of a data breach.[14] I therefore support the mechanism contained in the Bill that allows entities a reasonable amount of time to assess the breach before deciding whether to notify.

Section 26WC allows entities up to 30 days to carry out a reasonable assessment of whether there has been a serious data breach. This period starts when the entity becomes aware, or when the entity ought to reasonably have become aware, of the breach.

With time to make a reasonable assessment, entities will not immediately notify affected individuals and the Commissioner as a matter of course following a data breach. This may in turn also prevent notification fatigue.

The Commissioner will have power to require an entity to notify serious breaches

The OAIC supports the mechanism contained in s 26WD of the Bill that gives the Commissioner power to direct an entity to notify a serious data breach.

I believe that this mechanism accords with my other powers set out in the Privacy Act that are aimed at addressing serious interferences with individuals' privacy.

---

[13] As encryption is not fool-proof, the OAIC would not be supportive of a blanket exception to notification where the compromised information has been encrypted.

[14] Ponemon Institute, C*ost of a Data Breach Report 2015*, http://www-03.ibm.com/security/data-breach/, page 13.

Implementation of the Bill

If the Bill is enacted, the OAIC anticipates that entities covered by the scheme will look to the OAIC for guidance about how it operates.

The OAIC intends to develop and issue guidance material to help entities:

- assess whether a 'serious data breach' has occurred, and
- understand how to comply with notification requirements.

The OAIC will also update or replace its current voluntary DBN Guide.

In the past, in relation to privacy and freedom of information reforms, the OAIC has:

- provided general policy advice to agencies and organisations
- undertaken community education to encourage better privacy and government information practice, and
- conducted research to identify and address emerging privacy, freedom of information and government information policy concerns.

The OAIC is committed to taking what steps it can to provide support to government, business and the community if the Bill is enacted.

Conclusion

The OAIC continues to support the introduction of a mandatory data breach notification scheme.

If you have any questions about this submission, please phone Este Darin-Cooper, Director, Regulation and Strategy Branch, [contact details redacted].

Yours sincerely

Timothy Pilgrim
Acting Australian Information Commissioner

3 March 2016