Australian Government
Office of the Australian Information Commissioner

Julie Dennett
Committee Secretary
Senate Legal and Constitutional Affairs Committee
Parliament House
CANBERRA ACT 2600

By email: legcon.sen@aph.gov.au

Dear Ms Dennett

Inquiry into Privacy Amendment (Privacy Alerts) Bill 2013

Thank you for the opportunity to make a submission on the Senate Legal and Constitutional Affairs Committee Inquiry into the Privacy Amendment (Privacy Alerts) Bill 2013 (the Bill).[1] The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comments on the Bill for the Committee's consideration.

The OAIC supports the introduction of a mandatory data breach notification requirement. In this submission we outline the benefits of a mandatory data breach notification requirement, the current underreporting of data breaches in Australia, and the impact of the implementation of the Bill on OAIC operations and current resources.

Mandatory data breach notification

In its 2008 report *For Your Information: Australian Privacy Law and Practice*,[2] the Australian Law Reform Commission recommended that the *Privacy Act 1998* (Cth) (Privacy Act) be amended to impose a requirement on government agencies and private sector organisations covered by the Privacy Act (entities) to notify the Privacy Commissioner and affected individuals when:

- there has been a data breach of 'specified personal information', and
- that breach 'may give rise to a real risk of serious harm' (recommendation 51-1).[3]

The OAIC supports (and the former Office of the Privacy Commissioner supported) that recommendation. This is reflected in several public submissions by and publications from the OAIC (and the former Office of the Privacy Commissioner), including:

- *Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31*, February 2007[4]

---

[1] www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/privacy_alerts_2013/info.htm
[2] www.alrc.gov.au/publications/report-108
[3] www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/alrc%E2%80%99s-view

- *Submission to the Australian Law Reform Commission's Review of Privacy - Discussion Paper 72*, December 2007[5]
- the OAIC's current voluntary data breach notification guide, *Data breach notification: A guide to handling personal information security breaches,* first published in August 2008 and updated in April 2012[6]
- the OAIC's submission to the AGD discussion paper, *Australian Privacy Breach Notification*, December 2012.[7]

The OAIC was consulted by the Attorney-General's Department regarding the drafting of the Bill.

Benefits of data breach notification

The OAIC considers that a requirement that entities notify individuals when a data breach involves their personal information is desirable for a number of reasons.

Notification can help affected individuals to mitigate potential harm

Identity theft and personal fraud is an increasingly problematic issue in Australia. In the 2010/2011 financial year, personal fraud cost Australians $1.4 billion. Further, 1.2 million Australians aged 15 years and over were victim to at least one incident of identity fraud in that year; a significant increase from 806,000 victims in 2007.[8]

In some circumstances, notification can prevent or limit identity theft and personal fraud by helping to protect personal information against misuse, loss or unauthorised access, modification or disclosure. Specifically, where personal information has been compromised, notification can be essential in helping affected individuals regain control of that information and 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 identity information by changing passwords or account numbers, or requesting the reissue of identifiers. Such steps help prevent or limit the risks resulting from the theft of personal information.

Notification can be beneficial to entities that experience data breaches

There is evidence that the incidence of data breaches is increasing on a global scale and within Australia (see 'Underreporting of data breaches'). Further, the OAIC has observed

---

[4] www.oaic.gov.au/privacy/privacy-archive/privacy-submissions-archive/submission-to-the-australian-law-reform-commissions-review-of-privacy-issues-paper-31-february-2007

[5] www.oaic.gov.au/privacy/privacy-archive/privacy-submissions-archive/submission-to-the-australian-law-reform-commissions-review-of-privacy-discussion-paper-72-december-2007

[6] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

[7] www.oaic.gov.au/news-and-events/submissions/privacy-submissions/discussion-paper-australian-privacy-breach-notification

[8] Australian Bureau of Statistics, *Personal Fraud Survey for 2010-11,* www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument

increasing public concern about the way that personal information is handled by agencies and organisations, particularly with respect to data breaches.

The introduction of a mandatory notification requirement is an important signal to entities and to the public that the protection of personal privacy remains a priority in the digital age.

There can also be significant benefits to an entity when it notifies affected individuals that a data breach has occurred within the entity. Notification can help rebuild public trust and demonstrate to the public that the entity takes the security of personal information seriously, and is working to protect affected individuals from the harms that could result from a data breach.

In addition, there is evidence that prompt notification to affected individuals can help limit the costs associated with a data breach (including the costs derived from loss of reputation, remediation of the breach, and steps required to mitigate harm resulting from the breach).[9]

Underreporting of data breaches

Currently, entities covered by the Privacy Act are not expressly required to notify either the OAIC or affected individuals of a data breach under the Information Privacy Principles (IPPs: s 14 of the Privacy Act) or National Privacy Principles (NPPs: Schedule 3 to the Privacy Act). However, notification may be a reasonable step to protect personal information from misuse under IPP 4 and NPP 4; this is reflected in the OAIC's *Guide to Information Security*.[10] Further, s 75 of the *Personally Controlled Electronic Health Records Act 2012* (Cth) imposes specific mandatory notification requirements imposed on entities covered by that Act.

There is evidence that suggests that the incidence of data breaches is increasing globally and in Australia. For example:

- *The State of Privacy Awareness in Australian Organisations*, a study based on 500 interviews of representatives of Australian businesses commissioned by McAfee Australia and released in April 2013, identified that:
    - 21 per cent of Australian organisations interviewed had experienced a data breach, and
    - 14 per cent of organisations interviewed were unsure if they had experienced a data breach.

    Further, in instances of an admitted breach:

    - 18 per cent of organisations interviewed did not notify anyone outside the organisation of the data breach
    - 68 per cent did not notify affected customers of the data breach, and
    - 79 per cent did not notify affected suppliers of the data breach.
- In April 2013, documents tabled in the Canadian Parliament showed that since 2002, departments of the Canadian Federal Government had experienced 3,143 data

---

[9] Ponemon Institute; *Cost of a Data Breach Report 2012*, http://bit.ly/HoG3cL, page 9.
[10] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security

breaches, affecting over one million individuals. However, only about 13 per cent of the breaches were reported to the Canadian Privacy Commissioner.[11]

- Verizon's *Data Breach Investigations Report 2013* identified a global increase in data breaches caused by corporate and state-sponsored espionage, increases in breaches affecting financial institutions, larger organisations and professional services, and an increase in breaches committed by employees of affected organisations.[12]
- The *McAfee Threat Report for Q4 2012* noted that publicly reported data breaches (globally) have tripled since 2007.[13]
- IBM's *X-Force 2012 Year-End Trend and Risk Report* identified 1,502 events globally in which companies reported the loss of corporate data due to a leak or breach in 2012, a 40 per cent increase on the previous year.[14]
- The Ponemon Institute's *Cost of a Data Breach Report 2012* noted a marked increase in the costs of data breaches, globally and in Australia (for the fourth year running).[15]

Security industry commentators have reported that, in their experience, many breaches are not reported.[16] Further, under the OAIC's current voluntary notification scheme, in 2011-2012, the OAIC received 46 notifications between July 2011 and June 2012.[17] This is down from 56 notifications in 2010-2011.[18] Taken together with industry reports, this comparatively small number of notifications, and its recent reduction, leads the OAIC to believe that the incidence of data breaches in Australia is significantly underreported.

Implementation of the Bill

In November 2012, the Parliament passed the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (*Amendment Act). The Amendment Act introduces extensive amendments to the Privacy Act, the majority of which will come into force in March 2014. The Amendment Act has also prompted consequential amendments to a number of other pieces of privacy and related regulation.

---

[11] www.canada.com/urges+privacy+watchdog+probe+unreported+data+breaches/8307428/story.html#ixzz2ToU9MIPY

[12] www.verizonenterprise.com/DBIR/2013/

[13] www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf

[14] www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov12250

[15] http://bit.ly/HoG3cL

[16] See, for example, Sydney Morning Herald, *Not even fish 'n chip shops immune from leaking secrets*, 17 May 2012, www.smh.com.au/it-pro/security-it/not-even-fish-n-chip-shops-immune-from-leaking-secrets-20120517-1yrrf.html: *'According to consultant Marc Bown at IT security firm Trustwave, a company that investigates data breaches on behalf of banks, there were at least 60 unreported data breaches primarily concerning the theft of credit card information at Australian businesses last year. The surprising number is in addition to the 56 data breaches officially reported to the Privacy Commissioner in the* [2010/2011] *financial year.'*

[17] OAIC Annual Report 2011 -2012, www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201112/, page 64.

[18] 2009-2010 Annual Report of the Office of the Privacy Commissioner, www.oaic.gov.au/about-us/corporate-information/annual-reports/office-of-the-privacy-commissioner-annual-reports/200910-annual-report-of-the-office-of-the-privacy-commissioner, page 67.

The OAIC notes that entities covered by the Privacy Act have expressed some apprehension regarding how the various reforms operate, and have highlighted the need for clarity and timely guidance on the reforms. They look principally to the OAIC to provide that clear guidance. The OAIC is responding by giving priority to the development of critical guidance material, including:

- comparison guides between the Australian Privacy Principles, and the existing Information Privacy Principles and National Privacy Principles[19]
- a guide to information security (including what the OAIC considers to be the 'reasonable steps' that entities are required to take under the Privacy Act to protect the personal information they hold)[20]
- guidelines on the Australian Privacy Principles (which will shortly be released for consultation)
- the OAIC's voluntary *Data breach notification - A guide to handling personal information security breaches* (Voluntary DBN Guide).[21]

If the current Bill proceeds, the OAIC will prioritise the amendment of the OAIC's Voluntary DBN Guide to address and provide clarity on the operation of the new mandatory notification requirements.

Government and business also look to the OAIC to provide other support. In the past, for example, in relation to privacy and freedom of information reforms, the OAIC has provided general policy advice to agencies and organisations, has undertaken community education to encourage better privacy and government information practice, and has 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 a similar level of support to government, business and the community should the Bill be enacted. However, the OAIC's workload is currently exceeding its resources, and that workload continues to increase. For example, in the 2012/2013 financial year as at 31 May 2013, the OAIC had received:

- 1393 privacy complaints, compared to 1358 in the entire 2011/2012 financial year
- 472 Information Commissioner (IC) review applications, compared to 456 in the entire 2011/2012 financial year, and
- 140 FOI complaints, compared to 128 in the entire 2011/2012 financial year.

Secondly, there is a large and growing backlog in the OAIC's caseload. For example, at 31 March 2013:

- the oldest active IC review application on hand was 795 days old

---

[19] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/australian-privacy-principles-and-information-privacy-principles-comparison-guide

[20] See footnote 9.

[21] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

- the delay in allocating new cases was
    - 197 days for IC review applications,
    - 110 days for privacy complaints, and
    - 86 days for FOI complaints.

In that respect, we note that the OAIC has not been provided with additional resources to deal with this ongoing increase in its workload, or to implement the substantial changes and challenges associated with the Amendment Act. Further, the OAIC is subject to the Efficiency Dividend, which can markedly affect its capacity as a small agency to absorb new work and undertake some of the Tribunal-like functions it discharges in FOI and privacy work.[22]

We apprehend, in relation to the Bill, that the OAIC's ability to provide policy advice to agencies and organisations, conduct desirable research, and develop specialised guidance materials, could be impaired without additional resourcing.

We have also observed that entities are increasingly turning to consultants and law firms for advice on privacy and FOI issues. It may be that some of this cost could be avoided if the OAIC was better placed to provide additional guidance, advice, training and education.

Impact on OAIC operations

While the OAIC supports a mandatory notification requirement, we consider that the implementation of the provisions of the Bill will have a significant impact on the OAIC's workload and resources.

The OAIC will need to modify its existing workflow and document management systems to deal with the nature and volume of the notifications that will be required by the Bill; this will result in an increase in the OAIC's capital costs.

Following notification by an entity to the OAIC, there may be a need to investigate certain breach incidents. This may be necessary where a notification does not comply with the requirements of the Bill, where the details contained in the notification require verification, or where the OAIC holds the view that further action by the entity is necessary and appropriate.

Other aspects of the Bill that could have similar workload implications for the OAIC include:

- the Bill provides that entities that suffer a data breach may apply to the OAIC for an exemption from the requirement to notify affected individuals (s 26ZB (7)), and
- the requirement to notify affected individuals (s26ZB(1)) does not apply while the Commissioner considers an application for an exemption (s26ZB (9)(C)).

---

[22] See the letter from John McMillan, Australian Information Commissioner, to David Tune, Secretary, Department of Finance and Deregulation dated 2 February 2012, tabled in the Committee's Additional Estimates on 14 February 2012, available at http://resources.news.com.au/files/2012/03/26/1226310/517116-letter-from-the-information-commissioner.pdf

The OAIC anticipates these provisions, if passed, could be invoked in relation to many data breach incidents. In particular, there is a possibility that some entities that experience a data breach will apply to the OAIC for an exemption, which could have the result of transferring from the entity to the OAIC the decision as to whether the breach in question is a 'serious data breach' that requires notification under the Bill.

Finally, the OAIC notes that where entities fail to notify the OAIC and affected individuals in accordance with the requirements of the Bill, that failure will constitute an 'interference with privacy' within the meaning of the Privacy Act (s 13 of the Privacy Act as it will be amended by the Amendment Act) and will activate the investigatory mechanisms in the Act. Resources will be required to take enforcement action such as negotiating enforceable undertakings (s 33E), or making a determination. In addition, a failure to notify may attract a civil penalty (s 13G) necessitating action in the Federal Court.

Conclusion

The OAIC continues to support the introduction of a mandatory data breach requirement and will apply its available resources to implement any Bill passed to the extent possible.

We trust that these comments are of assistance to the Committee.

Yours sincerely

Prof. John McMillan
Australian Information Commissioner

Timothy Pilgrim
Australian Privacy Commissioner

20 June 2013