Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Senate Standing Committee on Legal and Constitutional Affairs

on

Privacy Amendment (Privacy Alerts) Bill 2013

20 June 2013

Contents

Office of the Victorian Privacy Commissioner (Privacy Victoria)
GPO Box 5057
10-16 Queen Street
Melbourne Victoria 3000
Australia
Phone: 1300-666-444
Fax: +61-3-8619-8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

1. Summary of submission

- The Acting Victorian Privacy Commissioner strongly supports the proposal to introduce data breach notification requirements, but:
    - The trigger to notify (a 'real risk of serious harm') is not clearly defined. The OAIC should be given legal authority to provide guidance to agencies about this requirement;
    - A rebuttable presumption in favour of notification should apply;
    - The ability for an entity to apply to the OAIC for exemptions may cause delay concerning notification unless the OAIC is provided with additional resourcing and a specific time period in which to determine exemptions; and
    - Small businesses remain exempt from notification, despite the possibility that there may be a 'real risk of serious harm' to individuals.

2. Introduction

I am grateful for the invitation from the Senate Standing Committee on Legal and Constitutional Affairs ('the Committee') dated 18 June 2013 to provide a submission to the Committee's *Privacy Amendment (Privacy Alerts) Bill 2013* ('the Bill') inquiry and report.

The short timeframe has limited my ability to explore the issues in detail. However, should the Committee require more information or have any questions on any particular issues I have raised, I would be more than happy to assist.

At the outset, I strongly support the proposal to introduce data breach notification requirements. As discussed in this office's previous submission to the Commonwealth Attorney-General's Department, there are significant benefits that flow from mandatory data breach notification requirements. These extend to the entities covered by the *Privacy Act 1988* (Cth) ('Privacy Act'), to individuals and to the regulator, the OAIC, by;

a. Providing individuals with the opportunity to mitigate the consequences of any breach relating to their personal information;
b. Acting as a strong incentive for organisations to improve data security;
c. Tracking incidents and obtaining statistical data as to the amount and extent of data security breaches;
d. Ensure individuals are confident engaging with organisations and Government when providing their personal information; and
e. Enabling the OAIC to identify patterns of non-compliance and to take proactive steps to assist entities to address current and emerging information privacy and security risks.[1]

[1] Privacy Victoria, *Submission to the Commonwealth Attorney-General's Department on its Australian Privacy Breach Notification Discussion Paper*, December 2012, available at http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/australian-privacy-breach-notification-discussion-paper

That said, the Bill contains several technical shortcomings that could limit the policy objectives it seeks to achieve. These are discussed below.

3. Summary of the proposals

The Bill establishes a regulatory scheme for data breach notifications to either affected individuals or the Privacy Commissioner ('Commissioner' or 'OAIC'):

- The scheme applies to entities regulated by the *Privacy Act* and that hold personal information;
- Those entities are required to take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure (Australian Privacy Principle (APP) 11.1);
- Where either unauthorised access, unauthorised disclosure or loss occurs, and the access/disclosure/loss will result in a **real risk of serious harm**, the access/disclosure/loss is a **serious data breach** of the APP[2]; and
- Where a **serious data breach** occurs, under proposed section 26ZB, an entity must prepare a statement ('notification') concerning the situation. It must take reasonable steps to notify the individuals significantly affected by the serious data breach, and also notify the Commissioner.

The Bill also sets out some inclusions and exceptions, being:

- It establishes that entities retain accountability for notification of serious data breaches where an entity has disclosed personal information to an overseas recipient under APP 8 (see section 26X(3));
- It contains specific provisions for credit reporting bodies (proposed sections 26Y and 26Z) and tax file number information (s 26ZA);
- An exception for enforcement bodies where compliance with the notification scheme would be likely to prejudice one or more enforcement related activities (s 26ZB(4)) and/or is inconsistent with secrecy provisions (s 26ZB(10)); and
- The Commissioner may exempt entities from notification if it is in the public interest (s 26ZB(5)), and including a process of application by entities to the Commissioner. Additionally, the Commissioner may also direct entities to perform notification (s 26ZC). Commissioner decisions are reviewable to the Administrative Appeals Tribunal.

Failure by entities to comply with the notification scheme constitutes an interference with an individual's privacy.[3] This means that it will be subject to the new and enhanced enforcement provisions provided to the Commissioner by the *Privacy Amendment* (*Enhancing Privacy Protection) Act 2012* (Cth).

[2] Note that proposed section 26X(2) of the Bill also extends the protection to loss of personal information "in circumstances where unauthorised access to, or unauthorised disclosure of, the personal information may occur" and that assuming that were to occur (i.e. unauthorised access/disclosure) would result in a real risk of serious harm to individuals to whom the personal information relates.

[3] Clause 3

4. What is a real risk of serious harm?

a) Lack of certainty around when entities need to notify

One potential area of uncertainty surrounds definitional questions concerning the circumstances that trigger the notification requirement. The requirement is that an entity believes on reasonable grounds that there has been a "serious data breach" concerning affected individuals, in turn defined as being that the disclosure/access/loss etc. will result in a "real risk of serious harm". As the notification requirements are predicated on the entity's (or Commissioner's) interpretation of this requirement, lack of clarity (or a means by which clarity can be achieved) may lead to entities either under-reporting or over-reporting security breaches.

'Harm' is defined at s 26ZE inclusively as including harm to reputation, economic harm, and financial harm, although presumably relying on the words' ordinary meaning, could extend outside of these types of harm. 'Real risk' is defined as a "risk that is not a remote risk" (s 26ZF). These two definitions alone may not be adequate for an organisation to determine when it is required (or not) to perform notification.

Further, and of particular concern, is the fact the term 'serious' is undefined. This, again, is a potential source of uncertainty or confusion. The *Explanatory Memorandum* goes some way to attempting to flesh out what 'serious harm' constitutes, mentioning physical and psychological harm, but is of limited legal force.[4]

b) Provide a power for the OAIC to produce guidelines on the definitional question

A mechanism that could be used to address these concerns would be to provide the OAIC with the legal authority to provide guidance on these issues. The OAIC's guidance may be able to provide direction about, and examples of, the kinds or types of harm that would meet the threshold. Although the *Explanatory Memorandum* indicates that this process will occur, my understanding is that any OAIC guidance will be merely persuasive.

Quite clearly, subsequent OAIC guidance will need to take into account different scenarios and contexts in which organisations handle personal information. There are a number of preexisting publications which may be of assistance in this process – examples include the OAIC's April 2012 *Guide to handling personal information security breaches.* I note that this (currently, voluntary) document does list considerations in determining harm,[5] but the Bill as it stands does not provide the Commissioner with a regulatory power to define these terms or provide the Commissioner's guidance any legal authority.

There are also a variety of other sources which may be used by the OAIC to inform the development of guidance. In the defence and law enforcement contexts, officials are often

[4] *Explanatory Memorandum,* p 2. For information as to the extent to which material in an extrinsic document can be taken into account by a court interpreting legislation, see Pearce and Geddes, *Statutory Interpretation in Australia*, 5th Edition, 2001, Butterworths Australia, Chapter 3 [3.1 – 3.46]

[5] For example, see pp 12-17 of the OAIC's *Guide to handling personal information security breaches* (April 2012).

required to report on serious security breaches and relevant agencies have produced internal guidance for their staff. This may be a potential source.

Any approach to resolving these issues should be consistent with the Commonwealth's *Protective Security Policy Framework* (PSPF), which details government expectations in relation to security incident management and reporting. The PSPF is a risk-based, administratively imposed protective security framework and, as such, ideally should be linked with and inform the OAIC's authority to produce mandatory guidance material.

Ultimately, the best way to determine the trigger for notification is not through abstract legislative definitions (irrespective of whether such definitions are exclusive or inclusive) but by the OAIC developing binding guidelines to flesh out these terms and providing the Commissioner with an ability to amend those guidelines as circumstances, harms and risks evolve. This process would require the OAIC to consult extensively with relevant stakeholders, but also with bodies tasked with policy and operational security responsibilities (in a Commonwealth context, this would include the Attorney-General's Department which has protective security policy responsibility.)

In summary, I recommend that the Committee consider whether the Bill should provide a power for the OAIC to issue legally binding guidelines as to precisely what constitutes a "real risk of serious harm." A model already exists in the *Privacy Act* – the ability of the OAIC to issue guidelines for handling of tax file numbers.[6]

5. Notification to the Commissioner

c) The Commissioner can exempt entities from notifications

Section 26ZB contains the requirement for entities to notify the Commissioner and individuals significantly affected. The Commissioner is provided with a power to exempt entities from notification (i.e. to affected individuals) under s 26ZB(5).

Section 26ZB(9) contains a mechanism where if any entity forms a belief about a serious data breach, and as soon as practicable after that belief, applies to the Commissioner for an exemption notice, the notification requirements do not apply for the period in which the Commissioner is making a decision in relation to the application.

d) Applications for exemptions may cause significant delays

Whilst I do not oppose providing the Commissioner with this power, I am concerned at potential practical effect of the provision. When an entity applies to the Commissioner for an exemption, the practical effect is that it 'stops the clock' on notification until the Commissioner has determined whether or not to grant an exemption. This could lead to a high level of applications to the Commissioner in circumstances where entities are either unsure of their obligation to notify (possibly due to uncertainty around the above definitions), or entities simply wish to try to escape or delay notification by applying for an exemption. At this point, the notification process enters a legal and administrative

[6] S 17 *Privacy Act 1988* (Cth). Under s 17(2), any guidelines issued are disallowable instruments as well, meaning a form of parliamentary oversight occurs.

lacuna and there is no mechanism available to remedy it. There is no obligation for the OAIC to determine such applications within a particular time frame.

This will impose a significant burden on the OAIC's processing and consideration of exemption applications. Any delay by the OAIC in determining applications for exemptions will result in a delay of subsequent notification to individuals (i.e. where an exemption application is rejected) thus exacerbating the potential risk of harm.

In my view, the policy objectives the Bill is designed to achieve would be more effectively implemented if there was a presumption in favour of notification. This would mean that an entity seeking an exemption should be required to satisfy the OAIC on the balance of probabilities that the exemption should be granted. Such a requirement should be subject to explicit time limitations and the OAIC should be empowered to withdraw an exemption where circumstances change.

e) The Bill should afford extra resources to the OAIC and contain a maximum time period for the OAIC to assess an exemption application

There is therefore a distinct possibility, given the lack of resources afforded to the OAIC and the lack of time limits in the Bill mandating the OAIC to make a decision within a particular time frame, of delay occurring in circumstances where there may be real risks of serious harm to affected individuals.

I suggest the Committee to consider:

- The potential resourcing implications on the OAIC in conferring additional functions on it;
- That the Bill provide a maximum time period in which the OAIC must make a decision to exempt/not exempt an entity from notification. If a decision is not made within that time period, the presumption in favour of notification would apply

6. Exempt organisations

f) Removal of the small business exemption for data breach notification

The notification requirements do not apply to organisations that are small businesses. My office (and the Australian Law Reform Commission) have recommended that the small business exemption be removed in its entirety. In my view the policy basis advanced to support the small business exemption from privacy does not apply to security and the exemption is accordingly misconceived.

In essence, the Bill's objective is to reduce harm that could occur to individuals by notifying affected persons of privacy and security breaches, and to manage risk. However, it is entirely possible that a significant data breach could occur in a small business context but, due to the exemption, that small business has no obligation to notify affected individuals.

The policy basis that underpins the small business privacy exemption is inapplicable to security. Small business makes up about 94% of Australian enterprises.[7] As the cost of information and communication technology has reduced and its capabilities have increased, more and more small businesses collect and handle large quantities of personal information. Trust in the security of personal information collected and handled by both the public and private sectors underpins the economic efficiencies that flow from the information economy. These efficiencies will be curtailed by exempting the vast majority of the private sector from any form of information security accountability.

David Watts
A/Victorian Privacy Commissioner

[7] Australian Law Reform Commission, *For Your Information – Australian Privacy Law and Practice Report*, Vol 1, Report 108 (May 2008) [39.1]