Australian Government
Attorney-General's Department

June 2013

Senate Legal and Constitutional Affairs Legislation Committee inquiry into the Privacy Amendment (Privacy Alerts) Bill 2013

Submission from Attorney-General's Department

Introduction

The Privacy Amendment (Privacy Alerts) Bill 2013 will amend the *Privacy Act 1988* (the Privacy Act) to introduce mandatory data breach notification provisions for agencies and organisations that are regulated by the Privacy Act. These entities will be required to provide notice to the Australian Information Commissioner and affected individuals of a serious data breach. That is where the data breach will result in a 'real risk of serious harm' to any affected individual, or where it relates to a data breach of prescribed personal information. Data breaches can result from hacking, theft or from internal errors or failure to follow information-handling policies that cause accidental loss or disclosure. More details about key aspects of the Bill are contained in the Explanatory Memorandum.

The Bill has a number of key aims.

First, it will be a key consumer protection and crime reduction measure. It will provide individuals who communicate with other through social media, or consumers who transact with companies online, with greater assurance that they can undertake those activities in a more secure and transparent environment. For example, it will allow individuals whose personal information has been compromised by a breach to take remedial steps to lessen the adverse impact that might arise from the breach such as identity theft and fraud (e.g by changing passwords, cancelling credit cards etc). As noted in the Regulation Impact Statement (RIS) in the Explanatory Memorandum to the Bill (p 8), studies from the United States indicate that there is empirical evidence showing that data breach laws contribute to decreases in identity theft rates.

Secondly, it will result in improved data security standards. It will act as an incentive to the holders of personal information to adequately secure information and be transparent about the handling of that information with individuals to whom the information relates, and the Office of the Australian Information Commissioner (OAIC). It is in the commercial interests of businesses to implement good privacy practices, because this leads to better customer relations, which leads to more business.

Thirdly, it will enable industry, consumers and regulators to have more information about data breaches; a better picture will form of what leads to breaches, either

accidental or malicious, and what measures and mitigations all parties can take to prevent or respond to breaches that do occur. This is important, not only to individuals who may suffer harm, but also because businesses that are targets of data breaches, particularly in the financial sector, often suffer financial loss as well.

Specific issues

The Department is aware of some specific issues that have been raised about the Bill. These are dealt with in more detail below.

Regulatory burden on business

A full RIS has been included in the Explanatory Memorandum (pp 4-35). It involved two major consultation processes involving a discussion paper and an Exposure Draft Bill. A range of stakeholders, including key industry groups, were invited to respond to specific questions about the possible regulatory burden on businesses from the scheme.

Based on that feedback, the Department's view is that, on balance, the creation of a mandatory data breach notification scheme will not raise significant cost or compliance issues for businesses who are currently preparing for the start of the major privacy reforms in March 2014. For these entities that are already in a position to comply with the OAIC's existing voluntary guide[1], there will be little, if any, change that they need to make to their systems. There will also be assistance for private sector organisations in preparing for the changes through the detailed guidance material that will be prepared by the OAIC as it revises its existing voluntary guide.

The specific cost impacts of the proposals on small businesses were considered in the RIS in the Explanatory Memorandum to the Bill. Most industry groups consulted did not identify a disproportionate impact on small businesses. Some identified small businesses that trade in personal information (who are subject to the Privacy Act) as entities that may incur adverse impacts more than other businesses. However, there was little evidence provided in support of this position, and the RIS therefore did not conclude that there would be any significant impact on small businesses.

[1] See OAIC Voluntary Guide at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

The Department acknowledges that entities are preparing to implement changes to transition to the new privacy reforms that will commence in March 2014, but the measures in the Bill are not likely to result in significant additional changes, particularly for those entities that are already compliant with the OAIC guide.

Concept of 'serious harm'

One of the key triggers is that the access or disclosure of personal information involved will result in a 'real risk of serious harm' to any of the individuals to whom the personal information relates (see, for example, subparagraph 26X(1)(d)(i)). This was the threshold recommended by the Australian Law Reform Commission in its recommendation on this issue[2], and is the current standard used in the OAIC voluntary guide. It is therefore a commonly understood concept amongst agencies and organisations that have sought to comply with the OAIC guide.

The term 'harm' has been defined in clause 26ZE to make it clear that it includes certain types of harm such as financial, economic, and reputational harm. That definition has been included because it may not be clear from the dictionary definition that these factors are meant to be considered when considering the issue of 'harm'.

The concept of what constitutes 'serious harm' is intended to be based on the same concept as currently appears in the OAIC guide. Entities have had no difficulties in understanding how it works under the guide. Rather than introduce uncertainty, it has flexibility to adapt the context in which an event occurs, as well as evolve over time. Accordingly, rather than seek to prescribe a definition in legislation, it is preferable that the OAIC develop guidance about the particular circumstances and factors that might be relevant to the question of harm. This is a common approach taken in privacy regulation, which is more principles-based in nature. It is intended that a revised OAIC guide will continue to provide guidance on the factors that entities should consider when assessing whether the harm is 'serious'.

Currently, the OAIC guide notes that harm could in some instances be 'serious' where it could lead to instances such as: identity theft, financial fraud, health fraud or fraud

[2] The ALRC's recommendation is at:
http://www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/alrc%E2%80%99s-view

against the Medicare and PBS systems. It could also be 'serious' where it could be used to create discrimination or disadvantage or, in extreme cases, blackmail.

Threshold for reporting data breach

Aside from the concept of 'serious harm', the other element of the key trigger noted above is that the risk to the affected individual from the data breach is 'real'. In terms of what would constitute a 'real risk', the Bill ensures that it excludes a risk that is a 'remote' risk (clause 26ZF). That is, a real risk cannot be something that is slight, unlikely, faint or improbable. That threshold is intended to exclude data breaches that are less serious and is intended to limit notification 'fatigue'. As with the existing OAIC guide, it is expected that a revised version of that guide will continue to provide practical guidance on the circumstances in which a 'real risk' may arise.

Regulations

The Bill provides for certain matters to be outlined in the regulations rather than the principal legislation. These regulations may be made in two circumstances.

First, regulations may be made to specify particular situations that may also be serious data breaches even if they do not necessarily reach the threshold of a 'real risk of serious harm' (e.g. subparagraph 26X(1)(d)(ii)).

For example, this could include the release of particularly sensitive information such as an individual's health information which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection. It is necessary to provide this flexibility because it may be apparent in the future that there are particular categories of personal information that require this higher level of protection.

Secondly, regulations will outline certain 'general publication conditions' which will outline the conditions under which an entity will be required to publish a notification about a serious data breach on its website and in newspapers, as opposed to directly contacting individuals (e.g. paragraph 26ZB(1)(h) and subclause 26ZB(12)).

There are a range of possible factors that might affect this issue, and which might differ depending on the entity involved, and the location of the affected individuals. The

making of regulations would enable more flexibility in allowing these matters of detail to be changed as notification processes develop into the future.

For example, the regulations could provide that the 'general publication conditions' are met:

- where particular individuals do not have readily available contact details, or
- where online and newspaper publication methods may reach a larger number of affected individuals in a more timely manner.

As would normally be the case with the development of privacy regulations, these would be prepared in close consultation with relevant stakeholders, including industry groups. In addition, any regulations made would also be an instrument subject to disallowance by the Parliament.

Order of action under existing OAIC guide

The Bill will not change the order of action that should be taken by entities in response to data breaches that currently comply with the OAIC Guide. The OAIC guide contains numbered steps to take in response to a data breach, but notes that particular steps may be taken simultaneously or in quick succession. Further, the OAIC guide states that immediate notification should be the *first* step if appropriate.

Therefore, the Bill does not have the effect of prioritising notification over other remedial action. The new notification requirement is completely consistent with the existing OAIC guide, and will complement existing legislative requirements that must be complied with in responding to a data breach.

In terms of other remedial action, the need to contain a data breach to protect against unauthorised access to, or disclosure of personal information, is an existing requirement in the Privacy Act (National Privacy Principle 4; Information Privacy Principle 4) which will continue under new Australian Privacy Principle 11.

Concept of 'loss'

The concept of 'lost' personal or other information (e.g. subclause 26X(2)) is intended to cover the situation where an entity has disclosed personal information inadvertently, or mislaid or left that information unattended (e.g. losing a laptop or USB). While that

information may never be accessed by an unauthorised person, it should still give rise to an obligation to notify because there is the potential for an unauthorised person to access the information. Early steps that are taken by individuals who could be adversely affected by that access could limit damage such as identity theft or fraud.

Currently, the OAIC Guide contains an example of where notification should occur where mail has been incorrectly sent to a different individual. For example, if the letter contains a PIN number, or contains health records, there may be a need to notify the affected individual. It is expected that a revised OAIC Guide will continue to provide practical examples to assist entities about this issue.