Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

4 May 2013

Supplementary Policy on Data Breach Notification Legislation

Introduction

It has been reported that the Australian Government is considering the introduction of data breach notification legislation. The APF makes the following comments on what is needed from Commonwealth legislation. These comments supplement the APF's Policy Statement on Data Breach Notifications, a copy of which is attached.

Generally, the APF welcomes action by the Commonwealth to create formal obligations that will expose inadequate data security practices, and provide individuals with information about mishandling of their data.

1. The Costs to Regulated Entities

Legislative proposals usually require regulatory impact information.

Requirements to notify data breaches, including the refinements we propose, are not punitive, or even expensive. They should all be regarded as a normal cost of doing business.

The costs of preventing breaches are in any case generally lower than the costs of handling them once they have occurred; and it is widely recognised that it is good business practice to proactively manage risks rather than to merely react when something goes wrong.

Further, the prevalence of mal-performance by organisations in relation to the security of personal data is so great that all of these requirements are justified.

APF's policy is that data breach notification requirements are warranted and are not unduly onerous.

2. The Title of the Legislation

APF's view is that, to avoid confusion, a Bill should use the conventional term 'data breach notification', and hence the title of a Bill should be something like 'Privacy Amendment (Data Breach Notifications) Bill 2013'.

3. The Scope of Applicability of Data Breach Requirements

Data breach notification obligations should not be limited to those organisations that are within the scope of the Privacy Act. This would be seriously inadequate. There is no justification for exempting from these provisions such organisations as small business enterprises, political parties, media organisations, and national security and law enforcement agencies. Nor is there any justification for exempting records that are exempt from the Privacy Act, such as data relating to employees.

APF's policy is that any legislation must apply to all organisations and all personal data that are reasonably within reach of Commonwealth jurisdiction.

4. The Nature of the Harm Caused

APF'S view is that the potential harm which can trigger data breach notification requirements, and the harm which is compensable, should clearly be of the widest possible ambit, and it should be clear that it is not limited to any specified categories such as harm to reputation, economic harm and financial harm. For example, the following need to be included:

- serious inconvenience without financial or economic harm occurring;
- onerous effort needed to right a wrong;
- unreasonable denial of a loan;;
- emotional distress, and psychological harm.

APF's policy is that it is essential that any law make clear that all forms of harm to individuals' interests must be taken into account.

5. The Trigger for Notification

The APF's view is that the trigger for notification must not be set at too high a risk of harm, and that risk of harm should not be the only trigger for notification (at least to the OIAC). Aggregation of terms limiting the nature of the harm that triggers notification increases the risk that organizations will argue that one or other aggregated term do not apply to them. For example, a phrase such as "real risk of serious harm" is a very high threshold, because of the combination of 'real' (i.e. 'not remote') risk, 'serious' harm (with no clear notion of seriousness) and 'harm' which may be given a limited definition (as discussed in 4. above).

In addition, a second trigger is necessary. Any significant breach should be subject to notification in any case. If that were not the case, then a significant insecurity would not become apparent, and would not be addressed, and it would be very likely that it would later give rise to a serious breach that was eminently avoidable. A single threshold test would result in a scheme which was a failure.

APF's policy is that a Bill should be based on either of two conditions being satisfied:
(a) a real risk of harm without qualifications such as 'serious'; OR
(b) a significant breach, whether or not real risk of harm has arisen.

6. Enforcement of Organisations' Security Responsibilities

If legislation is based on requiring notification only in the case of some, very serious breaches, then, although we understand the desire to avoid undue costs to organisations, and to avoid undue load on the OAIC, this means that the provisions will only have a very limited impact on organisations that have inadequate security safeguards. Hence two complementary features are necessary, as stated in the next two sections.

6.1 Clear Statement of Organisations' Security Responsibilities

In January 2013, APF submitted to OAIC, in relation to its revision of the Guide to Information Security, at http://www.privacy.org.au/Papers/OAIC-InfoSecy-1301.pdf, that:

(1) The OAIC's document needs to be revised to provide more direct guidance relating to the minimum safeguards that are required, together with references to documents that contain more detailed advice on specific security safeguards.

(2) The OAIC's document needs to be revised to make very clear that privacy-sensitive personal information must be subject to additional safeguards, well beyond the minimum safeguards, that address risks that arise in the particular context.

(3) The OAIC's document needs to be revised to project the following additional Key Messages, and provide supporting information:

- security safeguards are a mandatory requirement of the law, not optional;
- organisations that fail to implement the basic set of well-known safeguards for personal data are prima facie in breach of the Privacy Act, and are subject to enforcement actions; and
- organisations that handle privacy-sensitive personal information but fail to implement additional safeguards appropriate to the risks involved, are in breach of the Privacy Act, and are subject to enforcement actions.

APF's policy is that Data Breach Notification legislation needs to be complemented by clear and specific instructions by OAIC to organisations in relation to their obligations.

6.2 Non-Compliance to be an Interference with Privacy

Non-compliance with an obligation to notify needs to also be an 'interference with privacy', and to trigger the Commissioner's investigation and enforcement powers in the same way that other non-Principle breaches become actionable (e.g. of TFN Guidelines and credit rules).

The policy justification for this simple change is that, if this is omitted, then legislation would not empower individual data subjects who have been adversely affected by failure to notify a serious data breach to initiate any remedial action.

The proposed change would allow such individuals to lodge a complaint with the Commissioner concerning the non-compliance, and obtain any individual remedies to which they are entitled. Without such a provision legislation would be incomplete and insufficient in that it would rely completely on enforcement initiatives by the Commissioner, with no provision for individual data subjects to obtain a remedy. Such an approach is also necessary because non-compliance with data breach notification requirements would not necessarily be accompanied by any other breach of the APPs, so a data subject would not necessarily be able to make a complaint even though they have been very adversely affected by a failure to notify.

This would not impose any additional compliance costs on regulated entities.

APF's policy is that non-compliance with an obligation to notify needs to be an 'interference with privacy' and to trigger the Commissioner's investigation and enforcement powers.

7. Exceptions

Privacy legislation in Australia generally contains excessive exceptions which harm its effectiveness.

APF's policy in relation to any proposed exceptions is that:

- Any exemption should apply only to specific individuals;
- Exemptions should not apply to notification to the OAIC;
- Any organisation claiming exemption should be under an obligation to provide sufficient information to OAIC, or at the very least to a regulator such as the Inspector General of Security, in order to demonstrate compliance with exemption conditions; and
- Organisations should be under an obligation to notify as soon as the likelihood of prejudice that an exemption is aimed to prevent has expired.

8. Discretion for the OAIC

APF's policy is that no discretions should be given to the OAIC in relation to the operation of a data breach notification system; and that, if any is given, then it should be minimal, and should:

- **specify the precise circumstances in which it is available; and**
- **create an effective control over use of the discretion, such as publication of sufficient details that the public can evaluate the use of the provision.**

9. Publication of Data Breach Notifications by the OAIC

Some data breach notification schemes only require publications of notifications by the organisation concerned. The APF's view is that, whenever, publication of notification by an organisation is required, that notification should also be published on the website of the OAIC, and such notifications should be retained there permanently.

The principal policy reasons for this policy are that:

- Unless this aggregation occurs, most notifications will (i) never come to public attention because they do not fall under subsections (h) above; and (ii) even if they are published on a organisation's website, they will not be findable permanently after the event nor findable in the one location;
- It is important that all notifications, over time, be able to be browsed and searched, so that interested parties (and not only the OAIC) can identify any recurrent aspects of breach notification; and
- Transparency in data breach notifications is also likely to have a deterrent effect, and this is desirable.

The cost implications of compliance with this policy are negligible for organisations, because they would already be required to provide a copy of the notifications to be published to the Commissioner, and the cost of web republication by the Commissioner would be negligible.

APF's policy is that all serious data breach notifications must be required by the Act to be published on the Commissioner's website and retained there permanently.

10. Sanctions

APF's policy is that the new civil penalty provisions in the Privacy Act should be applicable where there has been a serious or repeated non-compliance with mandatory notification requirements. This is essential to ensure that compliance is not merely voluntary.

Australian Privacy Foundation

Data Breach Notification

APF Policy Statement on Data Breach Notification

A data breach occurs when personal data is exposed to an unauthorised person. It is a breach of trust by the organisation. It is commonly also a breach of the law. Unfortunately breaches of data protection laws are seldom subject to enforcement actions.

Data breaches occur remarkably frequently. Parliaments have failed to impose meaningful sanctions, and privacy oversight agencies have failed to exercise such powers and influence as they have to force organisations to ensure that appropriate security safeguards are in place.

In 2003, the Californian legislature responded to inadequacies in organisational practices by passing a Security Breach Notification Law. By 2006, 33 other US States had passed similar laws. Australian law reform has moved at glacial pace, and lags the US in this matter by a decade.

This document declares the APF's Policy on Data Breach Notification. It comprises the following sections:

Definitions

A **Data Breach** occurs where personal data held by an organisation has been subject to, or is reasonably likely to have been subject to, unauthorised access, disclosure, acquisition or loss.

A **Serious Data Breach** is a Data Breach that gives rise to a reasonable risk of harm to an individual.

A **Data Breach Notification** is a statement of the facts relating to a Data Breach.

The Purposes of Data Breach Notification

The purposes of Data Breach Notification are:

1. to inform the public, at a meaningful level of detail, about:
    - breaches
    - inadequacies in organisations' security safeguards
2. to inform individuals who have been affected by breaches, so that they can judge whether to:
    - take action to prevent or mitigate potential harm arising from the breach
    - seek compensation for harm caused
    - change their service-providers
3. to shame organisations that have seriously inadequate security safeguards into changing their ways
4. to encourage all organisations to implement adequate security safeguards

Data breach notification processes, guidelines and regulations need to be designed so as to achieve these purposes.

Organisations' Obligations in Relation to Data Security

1. All organisations must ensure that personal data is at all times subject to security safeguards commensurate with the sensitivity of the data. The APF has previously published a Policy Statement on Information Security
2. All organisations must take the steps appropriate in their particular circumstances to:
    - deter Data Breaches
    - prevent Data Breaches
    - detect Data Breaches
    - mitigate harm arising from Data Breaches; and
    - enable their investigation
3. All organisations must implement awareness, training and control measures to ensure appropriate practices by their staff
4. All organisations must conduct audits of security safeguards periodically, and when the circumstances warrant
5. All organisations must perform a Privacy Impact Assessment (PIA) when data systems are in the process of being created, and when such systems are being materially changed, in order to ensure that appropriate data protections are designed into their systems, and to demonstrate publicly that this is the case

---

Organisations' Obligations in Relation to Data Breach Notification

1. Conduct of an Investigation

Where grounds exist for suspecting that a Data Breach may have occurred, the organisation must conduct an investigation, in order to establish a sufficient understanding of the circumstances and the outcomes. The results of the investigation must be documented in a form that enables subsequent evaluation.

2. Submission of a Data Breach Notification

Where a Data Breach has occurred, or is reasonably likely to have occurred, the organisation must:

1. Submit a Data Breach Notification to the relevant oversight agency, in a manner consistent with the guidance issued by that oversight agency, as soon as practicable and without delay
2. Communicate sufficient information to affected categories of individual, the media, and/or representative and advocacy agencies, as appropriate to the circumstances

3. Form of a Data Breach Notification

A Data Breach Notification must include sufficient detail to enable the reader to achieve a proper understanding of the Data Breach, its causes, its scale, its consequences, mitigation measures, and the rights of individuals affected by it.

Details whose publication might result in harm or facilitate attacks on that or other organisations can be included within a separate Appendix whose distribution can be limited.

4. Additional Obligations in the Case of a Serious Data Breach

Where a Serious Data Breach has occurred, or is reasonably likely to have occurred, the organisation must, in addition:

1. Provide an explanation, apology and advice to each individual whose data is, or is reasonably likely to be, the subject of the Data Breach, as soon as feasible and without delay, but taking into account the possible need for a brief delay in the event that criminal investigation activities require a breathing-space
2. Publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information
3. Where material harm has occurred, provide appropriate restitution

4. Inform the oversight agency of the actions taken

The Reponsibilities of the Oversight Agency

1. Publish guidance in relation to data security safeguards.
This must make clear that organisations have obligations to perform Security Risk Assessment, and to establish an Information Security Risk Management Plan whereby information security safeguards are implemented and maintained, commensurate with the sensitivity of the data

2. Publish guidance in relation to Data Breach Notifications

3. In relation to Data Breaches:

- Liaise with organisations that have suffered Data Breaches
- Facilitate the Submission of Data Breach Notifications
- Inform the Public
- Publish the Data Breach Notifications in a Public Register

4. In relation to Serious Data Breaches:

- Review the outcomes of the organisation's internal investigation
- Where doubt exists about the quality of the internal investigation, conduct its own independent investigation
- Publish the results of the review and/or investigation
- Add details of the investigation into the Public Register

5. Facilitate improvements in organisational practices relating to data security

6. Facilitate remedies for individuals who have suffered as a result of Data Breaches

---

Enforcement

All obligations in relation to Data Breach Notification must be subject to sanctions and enforcement.

The sanctions applied must reflect:

- the organisation's degree of culpability, including:
  - the extent to which the organisation had implemented safeguards commensurate with the sensitivity of the data
  - the extent to which the threat(s) and vulnerability/ies that gave rise to the Data Breach were well-known or novel
- the promptness and effectiveness with which the organisation reacted once grounds existed for suspecting that a Data Breach may have occurred
- mitigation measures adopted by the organisation once it was apparent that a Data Breach had occurred, or was reasonably likely to have occurred
- any avoidance activities, misinformation or delays by the organisation in responding to the Data Breach and in its interactions with the oversight agency
- the scale of the Data Breach
- the sensitivity of the data that was the subject of the Data Breach
- the measures undertaken by the organisation in order to address the risk of recurrence of Data Breaches (as distinct from the organisation's statements about what it intends to do)
- to the extent that financial penalties are applied, the size of the organisation

---
