Australian Privacy Foundation

email: mail@privacy.org.au

web site : www.privacy.org.au

Australian Privacy Breach Notification Discussion Paper, October 2012

Submission to the Commonwealth Attorney-General's Department

November 2012

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public Inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably part of, a submission.

Background

In its 2008 report, *For Your Information: Australian Privacy Law and Practice,* the Australian Law Reform Commission (ALRC) recommended that the *Privacy Act 1988* (Cth) be amended to include a new Part requiring mandatory data breach notifications, when personal information has been exposed to an unauthorised person, and there is a real risk of serious harm[1]. The recommendations relating to data breach notifications were not addressed in the first stage of the Government's response to the ALRC report, released in October 2009, with consideration of this issue postponed to a second stage. The Discussion Paper released by Commonwealth Attorney-General's in October 2012 is the Government's

[1] ALRC 2008, *For Your Information*, Report 108 on Australian Privacy Law and Practice, Recommendation 51-1.

first step in responding to the data breach notification recommendations. This submission responds to the questions raised in the Discussion Paper.

Current position

Data breach notification has been addressed in guidelines released by the Privacy Commissioner/Office of the Australian Information Commissioner (PC/OAIC)[2]. The guidelines[3] set out the following four steps to consider in responding to a data breach or suspected breach:

- Contain the breach and do a preliminary assessment;
- Evaluate the risks associated with the breach;
- Notification;
- Prevent future breaches.

In relation to notification, the guidelines provide that this should be considered in the context of the particular circumstances of the breach. While the guidelines point out that notification may be an 'important mitigation strategy', they provide that whether or not a breach should be notified should be considered on a case-by-case basis.

In general, unless there is a suspected breach of the data security principle, or of the credit reporting provisions, the PC/OAIC has no power to investigate, or otherwise respond to, data breaches. Accordingly, compliance with the PC/OAIC guidelines is entirely voluntary. Moreover, the guidelines are pitched at a very high level of generality, providing data controllers with a high degree in flexibility in responding to data breaches, but little specific guidance.

We note that the PC/OAIC now regularly receives voluntary notifications – 46 in the 2011-2012 year, 56 in 2010-11 and 44 in 2009-10; but there is no way of telling what proportion of actual breaches this represents – it is reasonable to suppose that it is a small minority even of significant breaches (see below for discussion of 'significance' criteria). The Discussion Paper notes that in 2010-11 the Privacy Commissioner also opened 59 investigations into breaches of which there was no notification to the OAIC[4].

Introduction

The APF welcomes the government's decision to bring forward public discussion of this issue, which was previously relegated to the currently unscheduled second tranche' of the government's response to the ALRC report. APF has consistently argued that breach notification requirements should be introduced earlier rather than later. We submit that where breach notification requirements have been introduced overseas, they have provided a powerful stimulus to corporate attention to privacy compliance.

---

[2] Because of ill-advised amendments in 2010 there is now much confusion about the respective roles of the Privacy Commissioner (PC) and the Office of the Australian Information Commissioner (OAIC). For the purpose of this submission we use the joint acronym PC/OAIC – the necessary distinction can be made at the legislative drafting stage of any notification scheme.

[3] OAIC, *Data breach notification: A guide to handling personal information security breaches* (April 2012).

[4] The 2011-12 OAIC Annual Report confirms this figure, and 37 own motion investigation in 2011-12, although it is not clear that all of these OMIs in either year involved security breaches.

Unfortunately, through a combination of weak and ambiguous obligations, limited legal sanctions and lack of effective enforcement activity, privacy compliance has been a low priority in Australian boardrooms and government agency management teams. The absence of a body of privacy jurisprudence and of examples of significant penalties for non-compliance has made it very difficult for privacy officers and others with an interest in strong privacy compliance to sell the need for compliance measures as a priority even within regulatory/compliance teams, let alone as a wider governance and risk management issue.

This environment means that the value of mandatory data breach notification is even greater than it would be in a better functioning privacy regime. Nonetheless, while we would welcome a data breach notification scheme, we emphasise that it should not be seen a substitute for, or alternative too, a range of other improvements to privacy law and its implementation. Some improvements have just been enacted, but there are many others that are still needed in addition to breach notification.

Importance of case studies

We submit that well publicized case studies of breaches and how they have been responded to should be compulsory reading for senior managers in both the private and public sectors. The Privacy Commissioner has published reports on some of the better known Australian cases. We draw attention in particular to the breach, earlier in 2012, by the New Zealand Accident Compensation Commission (ACC). Presentations from ACC managers, including the CEO, and from the New Zealand Privacy Commissioner at a recent iappANZ annual conference[5] gave a comprehensive and candid insight into both the risk to organizations from privacy breaches and into how to respond to a breach – both what to do and what not to do. There may be other published case studies which would be equally valuable.

We suggest this both as an input to the government's further consideration of the issue, and also as an important component of any new requirement – it would be important that as many 'case studies' of actual breaches and resulting notifications as possible were made public, through the PC/OAIC.

Definitions and scope

A second general point relates to terminology (and scope). Around the world, 'data breach notification' has become the common generic description, and has been the term used in recent Australian debate, and practice (see for instance the Privacy Commissioner's Data Breach Notification Guide which adopted 'data breach' in its latest edition, replacing 'personal information security breach …' in an earlier version).

The Discussion Paper uses the term 'privacy breach notification' as well as 'data breach notification' without adequately exploring the significance of the wording. We can see both pros and cons in the two terms. 'Data' correctly connotes that the subject matter is personal information (the subset of privacy protected by the Privacy Act 1988, and similar State and Territory laws), rather than wider privacy

[5] See www.iappanz.org/

'breaches' or intrusions such as some other forms of surveillance. On the other hand, there is a risk that 'data breach is seen as synonomous with a security breach, which is arguably too narrow as the desirable scope for a mandatory requirement.

The Discussion Paper confirms its limited aspirations by suggesting notification as a possible requirement '…where certain types of personal information are accessed, obtained, used, disclosed to, copied, or modified by unauthorised persons.' (p.2).

While this reflects the ALRC's definition, it would seem to exclude three other categories of breach:

(a) inappropriate access, use or disclosure (i.e. contrary to use and disclosure principles) by authorised persons (this may involve another type of breach of the security principles such as IPP 4 or NPP 4 in the federal Privacy Act – APP 11 in the new scheme). We note that the definition of 'Data Breach' in the Privacy Commissioner's Guide is wider – '**Data breach** means, for the purpose of this guide, when personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse.'
(b) Breaches of data quality principles (such as IPP 8 and NPP 3, and the new APP 10) that arise for reasons other than a security breach.
(c) Breaches of other privacy principles, such as a failure to give proper notice to individuals, or excessive or unfair collection.

We assume that the proposed privacy breach notification scheme is intended to be to be limited to 'information privacy breaches, but not breaches in the third category (c) above. However, we submit that it should certainly cover breaches of types (a) and possibly (b), as well as the '… by unauthorised persons' category which is currently all that would appear to be proposed.

We submit that any mandatory notification scheme should use the term 'Data Breach' with the definition from the Privacy Commissioner's Guide as the basis, but possibly also including breaches of the data quality principle. We have used the term 'data breach' in this submission to have this meaning.

A wider scheme for IT security?

Another scope issue is the question of whether a data breach notification scheme should apply more widely to data breaches not involving personal information. We appreciate that this is beyond the scope of the Discussion Paper and of any likely scheme in the near future. However, we submit that many of the public interest arguments for data breach notification would apply equally to a much wider range of IT security breaches. We suggest that the government canvass the views of the IT industry, security professionals and all relevant government agencies about the value of a wider scheme. This consultation should not however delay development and implementation of a scheme for breaches involving personal information as an important addition to privacy law.

Key questions (posed in the Discussion Paper)

1. Should Australia introduce a mandatory data breach notification law?

1.1 Are the current voluntary data breach notification arrangements sufficient?

1.2 Should the Government introduce a mandatory data breach notification law?

The APF considers that individuals have a fundamental right to be informed of any data breach involving personal information about them. The right of individuals to be notified is not merely based upon the potential adverse consequences of the release of personal information, such as identity fraud, but is an aspect of personal autonomy[6]. As pointed out in the ALRC report, absent legal compulsion, data controllers have insufficient incentives to notify individuals of data breaches. In particular, the adverse reputational effects that follow from acknowledging data breach notifications are a powerful disincentive. The Discussion Paper sets out a number of additional rationales for mandatory notifications, including giving individuals the opportunity to mitigate harms arising from a breach and the incentives provided for improving data security. While important, the APF regards the rationales identified in the Discussion Paper as subsidiary to the right of individuals to be informed.

The OAIC's voluntary guidelines are not sufficient to deal with the problem of under-reporting of data breaches. The current guidelines are, in most respects, vague and ambiguous. They provide insufficient practical guidance, even for those seeking to comply. More importantly, voluntary guidelines fail to address the fundamental problem of insufficient incentives for data controllers to reveal unauthorised disclosures.

The main argument against mandatory notification laws is the potential cost imposed on data controllers. The APF considers that entities which collect and store personal information have fundamental obligations to be accountable to individuals for the security of that information, and to be transparent about dealings with the information, especially unauthorised releases. As pointed out by the ALRC, notification laws are desirable to 'improve accountability, openness and transparency in the handling of personal information by agencies and organisations'.[7] The cost of accounting for unauthorised disclosures should be seen as an inherent part of the collection and processing of personal information. Furthermore, in the electronic environment, the costs of informing individuals are far from prohibitive.

The APF does not consider that voluntary guidelines can ever provide sufficient incentives for data controllers to notify individuals of data breaches.

Accordingly, the APF supports the introduction of a mandatory data breach notification law.

[6] Reflecting Article 17 of the International Covenant on Civil and Political Rights to which the Australian Privacy Act gives effect.

[7] Amongst other reasons [ALRC Report 108, 51.47].

2. Which breaches should be reported?

2.1 What should be the appropriate test to determine the trigger for notification?

2.2 Should it be based on a 'catch all' test, or based on more specific triggers, or another test?

2.3 What specific elements should be included in the notification trigger?

An important feature of any mandatory data notification regime is the 'trigger' for notification. There are two aspects to this – the first is the definition of a breach which we have already discussed above. The second is the criteria of significance.

In relation to significance criteria, the APF agrees with the ALRC that the notification regime should be proportionate to the potential harm caused by a data breach.[8] In this respect, the Attorney-General's Discussion Paper points out that it may not be desirable for minor breaches to be notified because of the administrative burden placed on data controllers, the risk of notification fatigue by individuals and the lack of usefulness where mitigation is impossible.[9]

Applying the fundamental principle that individuals have a right to be informed of data breaches, the APF considers that the trigger for notification must not be set too high. Nevertheless, the APF acknowledges the potential costs of notifying minor breaches, and that individuals may become de-sensitised, or unduly alarmed, by over-notification. On the other hand, there is a real danger that imprecision in setting the trigger may be used to avoid disclosure. As the Discussion Paper points out, data controllers may well interpret a trigger based on the nature of 'harm' restrictively by, for example, confining it to the release of credit card information.

Applying a version of Solove's 'data abuse pyramid'[10], the APF supports a tiered notification regime, which includes mandatory notification of individuals where there is a risk of harm, but also imposes requirements, including notification of the OAIC where this trigger is not met.

First, the APF recommends the application of a 'catch-all' test whereby mandatory notification of affected individuals is triggered by a data breach, but only where there is a 'risk of harm' (Test B in the scheme we suggest later in this submission). In supporting this test, the APF notes that it applies a lesser threshold than the 'real risk of serious harm' test recommended by the ALRC. Given that the 'risk of harm' standard is subject to interpretation, the APF recommends that the OAIC be required to develop binding guidelines which provide more detailed standards, and which could include specific triggers.

Second, the APF accepts that there may be circumstances in which it may be difficult for a data controller to determine whether or not there has been a data breach. Accordingly, where an entity reasonably suspects that a data breach has occurred, and regardless of whether or not there is a risk of harm, the entity should be required to consider whether or not to notify affected (or potentially

[8] [51.48].
[9] Page 11.
[10] Daniel J Solove, "The New Vulnerability: Data Security and Personal Information" in Radin and Chander (eds) *Securing Privacy in the Internet Age* (2008).

affected) individuals of the potential data breach. Moreover, in those circumstances, the entity should still be required to report potential breaches to the OAIC.

The APF submits that entities be required to notify an individual where they have a reasonable belief that there is a significant actual or suspected data breach that poses a risk of harm to the individual.

The APF submits that entities be required to notify the PC/OAIC of any significant actual or suspected data breach (whether or not it poses a risk of harm).

3. Who should decide on whether to notify?

3.1 Who should be notified about the breach?

3.2 Which of the below should decide whether to notify?

(i) the organisation or agency;

(ii) the Commissioner; or

(iii) the organisation/agency in consultation with the Commissioner

The decision that a breach or suspected breach should be notified must inevitably rest with the entity concerned. It is however essential that entities are given detailed guidance as to the relevant criteria, and this should be provided through a combination of the law and supporting guidelines.

The APF submits that a breach notification scheme should involve several tiers of decision making and notification, without making the scheme unnecessarily complex.

We do not believe that the Privacy Commissioner (or OAIC) should be given a 'gatekeeper' role in relation to most 'notifiable' breaches – rather that is should play a 'backstop' reviewer role to ensure that entities are correctly applying the law and related guidelines.

Entities should be obliged to set up internal systems to report all actual or suspected data breaches to a designated officer. That officer should then be responsible for notifying all breaches or suspected breaches that pass a first test (Test A) to the OAIC, and separately initiate notification of affected individuals of any breaches that pass a second test (Test B), unless there are specified public interest grounds for not doing so (Test C).

The Privacy Commissioner should be responsible for advising any entity reporting a breach that in the entity's view passes Test A but not Test B if, in the Commissioner's view it does in fact pass Test B (but not Test C) and should therefore be notified to affected individuals. The Commissioner would also review cases where an entity had decided that a breach passed Test B but also passed Test C, and had therefore not initiated notification of affected individuals (see below).

Test A would be of **significance**. On receiving an internal or external report of an actual or suspected breach, and entity's designated officer would make (and document) a judgement as to whether the breach was significant enough to warrant applying Test B and C. The judgement would be based on application of Guidelines which the PC/OAIC would be required to develop and issue. All breaches that pass Test A should be notified to the PC/OAIC (after a judgement was made about Tests B & C).

Test B would be of **risk of harm**. The designated officer, taking advice as required, would decide if the actual or suspected breach posed a sufficient risk, or potential risk, of harm to at least some affected individuals. The judgement would be based on application of Guidelines which the PC/OAIC would be required to develop and issue. If the breach passed Test B, the entity would be required to initiate notification of affected individuals, as well as notifying the PC/OAIC.

The guidelines in relation to Test A and B would between them cover such matters as the sensitivity of the personal information involved in the breach. The categories of 'sensitive information' defined in the Privacy Act for the purposes of additional protection should be expressly considered in the guidelines, although we do not pre-judge whether they should automatically trigger either Test A or Test B. Other categories of information may be at least as 'significant' for the purposes of both tests, such as biometric information, which, if it falls into the wrong hands may pose a particular risk because it cannot be repudiated (c.f. a credit card number which can be cancelled and replaced).

The significance test (Test A) should not be a simple as for instance the mere number of affected individuals. A small release of sensitive information may be considered 'significant' while a larger volume breach, but only involving more trivial personal information, may not be. Because significance and risk of harm are so closely related, we anticipate that a single set of guidelines from the PC/OAIC would cover both Tests A & B.

Test C would be a **public interest in not notifying individuals**. The designated officer, at the same time as making their judgement on Test B, would consider if any of the specified public interest grounds for not notifying affected individuals applied. The judgement would be based on application of Guidelines which the PC/OAIC would be required to develop and issue, specifying relevant public interest grounds.

The breach notification scheme should operate independently from, and without prejudice to, the Privacy Commissioner's functions of complaint handling and own motion investigations, even where these involve security breaches.

4. What should be reported (content and method of notification), and in what time frame?

4.1 What should be the form or medium in which the data breach notification is provided?

Notification to the PC/OAIC should occur through a carefully designed web-form submission process. Notifications to affected individuals, where applicable, should generally use the normal form of communication between the organisation and its clients, provided this meets applicable security standards. In the majority of cases, communication is likely to be via email, and should not therefore involve significant cost.

4.2 Should there be a set time limit for notification or a test based on notifying as soon as is practicable or reasonable?

There must be strict time limits for most notifications, with any exceptions or extensions subject to clearly defined criteria. Initial notification to the PC/OAIC should generally be within 48 hours of an entity's designated officer becoming aware of the actual/suspected breach. Notification of affected

individuals, where applicable, should generally be within 5 calendar days of the decision (whether by the entity or by the PC/OAIC on review) that notification of individuals is required. The APF would expect that in many cases, notification of affected individuals could take place much earlier.

4.3 What should be the content of the notification?

Where an entity decides that a breach or suspected breach has passed Test A, notice to the PC/OAIC should include an initial assessment of:

- the nature of the personal information involved in the breach – usually by reference to 'plain english' descriptions of relevant database fields;
- the date and time on which, or period over which, the breach occurred;
- the potential impact of the breach including any risk of harm to affected individuals;
- the scale of the breach – e.g. was the entire customer base affected, or only users of one product or service;
- why the breach occurred – e.g. was it due to out of date software, or human error; remedial action taken to date:

and, where the entity has decided notification of affected individuals is not appropriate:

- a justification of that decision, on the basis of Tests B or C

Notice to affected individuals, where applicable, should include all of the same information as is notified to the PC/OAIC, and in addition:

- 'Plain English' information about any action that can be taken by the individual to minimise any risk of adverse effects, including links to relevant websites,
- A clear explanation of the rights of the individual to lodge a complaint under the Privacy Act or other relevant laws, including links to relevant websites and other contact details.

Notices both to the PC/OAIC and, where applicable, to affected individuals should be required to be updated periodically where significant fresh information becomes available.

5. What should be the penalty for failing to notify when required to do so?

5.1 Should there be a penalty or sanction for failing to comply with a legislative requirement to notify?

5.2 If so, what should be the penalty or sanction, and the appropriate level of that penalty or sanction?

There must be significant financial penalties for non-compliance, especially as the design of the scheme will place the onus on entities experiencing breaches to make the threshold decisions. The corollary of this 'light touch' regime (as opposed to mandatory reporting, at least to the PC/OAIC of *all* breaches) is the need for strong sanctions against any entity which deliberately evades the objective of the scheme by blatantly mis-applying the Tests. The PC/OAIC should also publish a list of entities that have been found to have breached their obligations under a mandatory data breach notification scheme. This would ensure both financial and reputational incentives for compliance.

The penalty scheme should be modelled on the new Privacy Act scheme as recently amended.

6. Who should be subject to a mandatory data breach notification law?

6.1 Who should be subject to a mandatory data breach notification law?

6.2 Should the scope of a mandatory data breach notification law be the same as the existing scope of the Privacy Act?

All APP entities (those with obligations under the Privacy Act) should be subject to any new mandatory data breach notification scheme. The ALRC recommended a review of existing exemptions and criticised 'blanket' exemptions. APF submits that any exceptions to any of the obligations under privacy law – including any new data breach notification scheme – should be specific, limited, clearly justified and in most cases conditional.

There are good arguments for applying a data breach notification scheme to many of the entities currently exempt, in whole or part, from the Privacy Act (such as small business organisations, political parties, media organisations engaged in journalism etc). Some of these require detailed further discussion and to avoid delaying introduction of a data breach notification scheme, it should initially have the same scope as the Privacy Act, with the issue of exceptions and exemptions to be addressed at the same time as for those applying to other Privacy Act obligations.

7. Should there be an exception for law enforcement activities?

7.1 Should there be an exception for law enforcement activities?

7.2 Would such an exception add anything to the ALRC's proposed public interest exception?

There should be no blanket exception from any data breach notification requirements for law enforcement activities, and no exception at all from the requirement to notify the PC/OAIC of *all* significant breaches.

There should be a limited set of criteria for exceptions to the requirement to notify affected individuals where another public interest substantially outweighs both the individual and public interests in individuals being notified. One such criterion would be where notification of affected individuals would significantly hinder a law enforcement investigation. This might include both active investigations by law enforcement agencies and, subject to strict conditions, preliminary investigations by the entity concerned prior to any referral to a law enforcement agency.

The PC/OAIC should issue guidance about the criteria for entities to make a decision not to notify individuals (Test C in the scheme we have suggested above). Such decisions would be subject to review by the PC/OAIC.

The public interest decision (Test C) should be one for the relevant entity to make in initially. They may take into account the views of any other entities that are involved (e.g. a law enforcement agency), and from the PC/OAIC but should not take directions from them to NOT notify (unless required by law to do so). The PC/OAIC would however have the power to direct an entity to notify affected individuals,

overriding the entity's decision that Test C applied, having taken into account both the reasons given by the entity and representations from any other interested party.

Passing Test C should not be a once and for ever decision. Individuals are entitled to be informed as soon as practicable about *any* significant breach that posed a risk of harm to them. An entity's designated officer should be required to periodically review breaches that had passed Test B and Test C to assess whether the grounds for passing Test C (and therefore not notifying affected individuals) still applied. If the grounds no longer applied, the entity should initiate notification of affected individuals – however long since the breach occurred and whatever remedial action had been taken.

Other matters

Register of Notifications

APF submits that the PC/OAIC should be required to maintain a register of notified breaches. To avoid deterring entities from reporting breaches, entries in the register which were of significant breaches not posing a risk of harm would not be public. Where, however, breaches passed Test B, but not Test C, and therefore triggered notification of affected individuals, specified details should be made public. Breaches which passed Test B and also Test C, justifying NOT notifying affected individuals, would be included in the non-public section of the Register (until such time as the justification for non-notification no longer applied).

The PC/OAIC should be required to publicly report regularly (more often than in an Annual Report) on the number and type of notifications, including those in the non-public sections of the Register.

For further contact about this submission:

Nigel Waters,

Board Member

board5@privacy.org.au

0407 230 342

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory