COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Daniel Thompson, Isaac Lin, David Ng, Moses Kakaire ISSN 08117225

Number: 88 February 2015

When there is a breach – Know your obligations and what steps to take

By David Smith and Tim Lee

David Smith *is a partner with Corrs Chambers Westgarth.*

Tim Lee *is an associate with Corrs Chambers Westgarth.*

Introduction

Data security is an increasing concern for organisations of all sizes. In order to comply with increasing layers of regulation and remain competitive in today's rapidly-moving, information-based economy organisations are now required to handle a greater variety and amount of personal information than ever before. However, as the "data footprint" of an organisation grows, so do the risks associated with data security breaches and the mishandling of personal information.

The recent proliferation of high-profile data breach incidents both in Australia and abroad has heightened consumer awareness of data security issues and renewed the debate about the value of mandatory data breach notification laws. One of the first questions for an organisation faced with a data breach is whether it should notify the affected individuals and/or the privacy regulator.

This paper reviews the current regulatory framework for data breach notifications under the *Privacy Act 1988* (Cth) (the Privacy Act) and considers how organisations should approach the tasks of determining whether notification is an appropriate response. We also discuss the potential introduction of mandatory data breach reporting in Australia through the *Privacy Amendment (Privacy Alerts) Bill 2014* (Cth), and briefly consider the experience of other jurisdictions that have introduced mandatory data breach notification schemes.

What constitutes a "data breach"?

The term "data breach" is not found in the Privacy Act 1988 (Cth) and does not have a settled definition in Australia law.

In this issue

From the editors…

In this issue, David Smith and Tim Lee consider the practical implications of data breach notifications by Australian organisations in light of the current privacy regime which does not explicitly mandate such notifications, proposed mandatory data breach notification laws in Australia and the experience of other jurisdictions where such laws exist.

John D Fitzgerald introduces us to the use of graph theory – the mathematical study of the collection of things related in some way to one another – in legal interpretation, and provides a demonstration by applying it to the structure and definitions of the *Health Practitioner Regulation National Law 2009* (NSW).

Finally, Pamela and Xenogene Gray explore the potential for better governmental administration and decision-making via the use of computerised logic systems capable of mapping complex rule systems and automating their application to a specific case. Their article illustrates how the superexpert shell eGanges in particular could have been used as a quality control tool to improve outcomes under the former federal government's home insulation scheme.

The Editors
Daniel Thompson, Isaac Lin, David Ng and Moses Kakaire

The Office of the Australian Information Commissioner (OAIC)[1] adopts the following definition in its *Guide to Handling Personal Information Security Breaches*[2] (Data Breach Notification Guide):

> "Data breach means, for the purpose of this guide, when personal information held by an agency or organisation is lost or subject to unauthorised access, use, modification, disclosure, or other misuse."

This definition reflects the language of Australian Privacy Principle (APP) 11 (formerly National Privacy Principle 4 and Information Privacy Principle 4), which requires organisations to take "reasonable steps" to protect personal information they hold from:

- misuse, interference[3] and loss; and
- unauthorised access, modification or disclosure.

This raises two important points about the concept of a "data breach". The first is that a "data breach" is not necessarily a breach of the APPs – rather, the word "breach" refers to the breach of the organisation's information security. Whether this security breach is a breach of the APPs will depend on whether the organisation's information security measures were sufficient in light of APP 11. Given this distinction, many organisations now choose to use language that more specifically describes the nature of the incident and which avoids connotations of fault – for example, "security incident".

The second important point about the definition is that it is not limited to malicious actions, such as theft or "hacking" (although the term "data breach" is commonly used to refer to such actions). It also includes situations where an organisation's mishandling of personal information results in misuse or accidental loss or disclosure (e.g. sending correspondence to the wrong address).

The Data Breach Notification Guide provides the following examples of situations that could give rise to a data breach:

- lost or stolen laptops or paper records containing personal information;
- databases containing personal information being hacked into or otherwise illegally accessed by external parties;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins; and
- an organisation mistakenly providing personal information to the wrong person.

In addition to these examples, a number of the OAIC's recent data breach investigations have concerned situations where networked records were stored on a publically accessible web server that did not have appropriate security controls and became discoverable via search engines. Recent examples include Multicard Pty Ltd (May 2014)[4], Telstra Corporation Limited (March 2014)[5] and Medvet Science Pty Ltd (July 2012)[6].

Is notification mandatory?

There is no specific obligation in the Privacy Act that requires an organisation to notify affected individuals (or the OAIC) of a data breach.

However, the OAIC considers that a requirement to notify affected individuals may form part of an organisation's general data security obligations under what is now APP 11.1. The Data Breach Notification Guide summarises the OAIC's position in the following terms:

> "*(R)easonable steps [to protect personal information under what is now APP 11.1] may include the preparation and implementation of a data breach policy and response plan. Notification of the*

> *individuals who are or may be affected by a data breach, and the OAIC, may also be a reasonable step.*" (This is because notification may give the individual the opportunity to minimise the risks of misuse etc. of the personal information.)

Notwithstanding the above, generally speaking mandatory data breach notification requirements do not form part of the Privacy Act regime. The Data Breach Notification Guide clearly states that compliance with the Guide is not required by the Privacy Act. We would expect that if the OAIC decides to take a firmer stance on enforcing its expectations regarding data breach notification using APP 11.1, it would first revise the Data Breach Notification Guide to remove the Guide's non-binding status (and to update it to refer to the APPs).

It seems more likely that if mandatory data breach notification requirements are to be introduced in Australia, it will be through legislation. The OAIC has expressed its support for a legislative solution and has given no indication that it intends to change its current position on data breach notifications. We consider the potential for legislative reform in section 6 below.

When should organisations consider notifying?

The Data Breach Notification Guide makes it clear that the principal question in relation to notification is whether to notify the affected individuals. A secondary question is whether to notify the OAIC (or others, e.g. the police).

There are a number of reasons why an organisation might consider notifying affected individuals in response to a data breach. If the matter is likely to become public, for example, there may be commercial and public relations incentives for quickly notifying affected individuals. Alternatively, the organisation may be bound by contract or specific industry codes to inform affected individuals. This will largely turn on the particular circumstances of the organisation and the nature of the data breach, which are fact-specific and beyond the scope of this paper.

From a "good practice" point of view (and possibly a Privacy Act compliance perspective), the Data Breach Notification Guide suggests that notification is only required when there is a "real risk of serious harm" to the affected individuals if notice is not given.

Interestingly, the Data Breach Notification Guide specifically discourages organisations from over-reporting minor breaches:

> "*Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals tonotice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.*"

This makes it clear that individuals should not expect to be informed about all data breach incidents.

From a practical perspective, it would therefore seem that a threshold question for the organisation to consider whether it is able to fully contain the breach and neutralise the potential risks created by the data breach. In such situations the organisation would not only be within its rights not to notify the affected individuals, but it would also be complying with the guidance of the OAIC.

The situations in which this principle would apply are probably quite narrow. An example might be where a security flaw is identified and resolved before it can be exploited (and the organisation is able to confirm that it has not been exploited). Another example provided in the Data Breach Notification Guide is where a pathologist sends test results to the wrong GP. Once the pathologist has spoken with the GP and asked her to destroy the test results, the pathologist can rely on the GP's professional duties of confidence as a justification for not notifying (and potentially, unnecessarily alarming or confusing) the relevant patient. A further example given by the OAIC is that if a laptop containing adequately encrypted information is stolen, but is subsequently recovered and investigations show that the information was not accessed, copied or otherwise tampered with, notification to affected individuals may not be necessary.

If the organisation is not confident that it is able to fully contain the data breach and its effects, the organisation should then consider whether there is a "real risk of serious harm" to the affected individuals if notice is not given.

Unfortunately, the Data Breach Notification Guide does not provide a clear test for determining when there is a "real risk of serious harm". Unlike the data breach notification regimes in other countries, the Guide does not provide any minimum "trigger points" in terms of number of affected individuals, or specific types of information (e.g. credit card details, health records). The OAIC is also yet to provide firm guidance on the extent to which data protection technologies (such as encryption) may influence the risk assessment for notification purposes, although it does make the comment in the Data Breach Notification Guide that over time, encryption algorithms may be broken.

Under the Data Breach Notification Guide, organisations are simply advised to consider a range of factors including:

- what types of harm the affected individuals could potentially be exposed to (e.g. identify theft, financial loss, threat to physical safety or emotional wellbeing, humiliation, reputational damage);
- whether notification would assist the affected individual to mitigate possible harm (e.g. by changing passwords) or prepare themselves in the event that sensitive or potentially embarrassing information has been released; and
- whether there are any legal or contractual obligations to notify (or not to notify, as the case may be – for example, an organisation may be directed by law enforcement agencies not to notify affected individuals where doing so might

prejudice an on-going investigation into the breach).

It therefore appears that organisations have fairly broad discretion to judge whether notification is appropriate, provided that they have a reasonable basis for their decision. In the absence of prescriptive guidance from the OAIC, organisations should probably be guided primarily by common sense and what seems reasonable in the circumstances (taking into account the affected individuals' legitimate interest in being informed of a data breach that could put them at risk).

One point that arises from the OAIC's investigation reports is that when an organisation is considering whether there is a "real risk" of "serious harm", the organisation must turn its mind to:

- whether the information was simply exposed, or whether it was viewed and/or copied;
- how many times the information was viewed and/or copied; and
- who could have viewed/copied the information, and what they are likely to do with the information.

It therefore appears that in a situation where the identity and motives of the person(s) behind the data breach are unclear, or where the information is of a sort that can be readily misused (e.g. financial information, passwords), the case for notifying affected individuals is stronger.

Further guidance can be taken from the Data Breach Notification Guide's list of information that should be included in a data breach notice:

- Incident description;
- Types of personal information involved;
- The organisation's response to the breach;
- What assistance the organisation can offer to the individual;
- Other sources of information that may assist individuals in mitigating the risks;
- The organisation's contact details; and
- Whether the Organisation has notified the OAIC.

(The OAIC also suggests that a data breach notice should include details of how an individual can lodge a complaint with the entity affected by the data breach, and also with the OAIC. We query whether it is actually in the entity's interest to inform the individual how to complain to the OAIC.)

It is clear from this list that a data breach notice should only be sent if it will serve a practical purpose and assist the affected individual to protect themselves from harm. A perfunctory "form" notice is not required, and should be avoided.

The OAIC also recommends that a data breach notice should only be issued after the organisation has:

- Completed its risk assessment and determined that notification is appropriate;
- Obtained as complete a set of facts as possible; and
- Carefully considered the legal implications of issuing the notice (including by seeking legal advice if necessary).

Organisations should avoid rushing to issue data breach notices. Recent examples of major data breaches have demonstrated the pitfalls of notifying before all the facts have been gathered – namely, reputational damage and consumer confusion. On the other hand, if affected individuals' interests are imminently threatened (e.g. their credit card numbers have been hacked), it will be important to work through the above considerations very quickly so that notification can, if required, occur quickly. The OAIC's position is that in some cases it may be appropriate to notify individuals immediately, even before containment or assessment of the data breach occurs.

In considering a data breach and how to respond to it, organisations should take into account that a breach that may initially seem minor many have major ramifications when the full implications are considered. An organisation's response needs to be carefully considered.

If a law enforcement agency is investigating, or likely to investigate, the data breach, consulting with the agency before making the details public may be prudent.

Who should be notified?

The Data Breach Notification Guide is primarily focused on notifying the affected individuals (as discussed above). However, the Guide also recommends that organisations should consider notifying the OAIC and other parties who may be affected by the data breach.

Self-reporting to the OAIC

The OAIC recommends that organisations should self-report serious data breaches (where there is a "real risk of serious harm" to the affected individuals) to the OAIC. This is the same test used to determine whether affected individuals should be notified.

The OAIC particularly recommends that organisations should self-report where the data breach is likely to attract a "high level of media attention", or where there is a reasonable expectation that the OAIC may receive complaints or enquiries about the breach (although these are probably just examples of "serious data breaches").

We suggest that where an organisation is notifying affected individuals, it would be sensible for the organisation to also notify the OAIC (especially given that the applicable test, a "real risk of serious harm", is the same). Self-reporting to the OAIC gives the organisation the chance to put its explanation of the incident to the OAIC first, and potentially persuade the OAIC not to open an own-motion investigation.

The Data Breach Notification Guide provides guidance on what information should be included in a notification to the OAIC. This includes a description of the breach, the types of personal information involved and a summary of the organisation's response.

Other parties to consider notifying

The Data Breach Notification Guide recommends that organisations should consider notifying the following parties if appropriate in the circumstances:

- Police;
- Insurers (or other parties if required by contractual obligations);
- Credit card companies, financial institutions or credit reporting agencies (if their assistance is necessary for mitigating the data breach);
- Government agencies that have a direct relationship with the compromised information (e.g. the ATO for tax file numbers or Medicare Australia for Medicare numbers);
- Professional or other regulatory bodies such as the ACCC, ASIC or ACMA (if required under professional or regulatory standards);
- Third party contractors who may be affected by the breach; and
- Relevant internal business units within the organisation that may not be aware of the breach.

Notification – potential reform

The introduction of mandatory data breach notification requirements has been recommended by the OAIC[7] and the Australian Law Reform Commission[8], and the concept has political support from Labor and the Greens. A recent survey conducted by the OAIC suggests that the idea of mandatory data breach notification attracts strong support from the Australian public[9]. The introduction of mandatory data breach notification obligations in Australia at some point in the future is therefore a distinct possibility. However, such reforms are not on the current Federal government's legislative agenda.

At the time of writing this paper, there is a private member's bill before the Federal Senate that would introduce mandatory data breach notification requirements if passed. The current Coalition Federal government confirmed during the bill's second reading debate on 19 June 2014 that it will not support the bill, although the Government did express support "in essence"[10] for the aims of the bill.

The *Privacy Amendment (Privacy Alerts) Bill 2014* (Cth) was introduced into the Senate on 20 March 2014 by Labor senator Lisa Singh (parliamentary secretary to the Shadow Attorney-General Mark Dreyfus). The bill had previously been introduced in 2013 by the then Labor Federal government. The 2013 version of the bill was passed by the House of Representatives but lapsed in the Senate following the change of government at the 2013 federal election.

If passed, the bill will require organisations to notify the Privacy Commissioner and affected individuals where the organisation believes on "reasonable grounds" that there has been a "serious data breach". The Privacy Commissioner will also have the power to compel an organisation to notify affected individuals if the Commissioner believes on reasonable grounds that a serious data breach has occurred. Failure to comply would constitute an "interference with the privacy of the individual" (that is, a breach of the Privacy Act), which can attract civil penalties of up to $1.7 million in serious cases.

The bill defines a "serious data breach" as any loss of, unauthorised access to, or unauthorised disclosure of personal information, credit reporting or credit eligibility information that results in a "real risk of serious harm". A "real risk" is a risk that is not remote, and "harm" includes reputational, economic and financial harm. Interestingly, the bill does not refer to the concepts of "interference" and "misuse" from APP 11.1.

The bill has been criticised as lacking clarity around the key concepts of "serious data breach" and "serious harm", which could create uncertainty for organisations (and the OAIC) in applying the "reasonable grounds" test. There is some merit to this criticism. While it could be said that the bill largely reflects the OAIC's current approach to data breach notification in that it gives organisations broad discretion to determine whether and when to notify, this level of scope for interpretation is probably unhelpful where notification is mandatory and there are potentially significant penalties for non-compliance.

On the other hand, if the trigger for notification is drafted too specifically this may encourage organisations to apply the test rigidly, which could result in "over-reporting" of data breach incidents and "notification fatigue" on the part of data subjects. Research from jurisdictions with mandatory notification triggers (in particular the United States) certainly suggests that this is the case. Concerns have also been raised about the compliance burden that a rigid notification system would impose on business. A formulaic approach to data breach notification fails to take into account the existing commercial and reputational incentives for organisations to notify affected individuals in the event of a serious data breach incident.

While the notion of mandatory data breach notification has a certain logical appeal, it may be difficult to develop a suitably robust model that balances regulatory certainty with appropriate flexibility.

Generally speaking, the issue of data breach notification has not featured prominently in the OAIC's investigations into data breach incidents to date. The OAIC's analysis is more focused on the sufficiency of the organisation's information security practices – even if the data breach response is appropriate, the organisation may still be found to have breached APP 11 by failing to prevent the breach[11]. As noted above, the OAIC technically already has jurisdiction under APP 11 to sanction a failure to notify where notification could have prevented harm. This somewhat weakens the argument that mandatory data

breach notification laws are required to address a "gap" in the current Privacy Act regime.

Practical tips to prevent data breaches and their consequences

Review your information security practices

The best way to prevent a data breach is to have suitably robust information security practices (including appropriate levels of training and governance).

A detailed discussion about what constitutes adequate information security for the purposes of APP 11.1 is beyond the scope of this paper, but the following comments can usefully be made based on recent OAIC decisions on data breaches:

- the OAIC expects that entities will be "fully aware of all the personal information they handle, where it is kept and risks associated with that information"[12];
- organisations are expected to proactively manage the activities of third party service providers that store and handle personal information on the organisation's behalf[13];
- a common area of vulnerability for many organisations is the failure to promptly delete or de-identify personal information that is no longer necessary (as required under APP 11.2)

The OAIC suggests that the reasonable steps (as required by APP 11.1) necessary to secure personal information will depend on context, including:

- the sensitivity (having regard to the affected individuals) of the personal information;
- the harm that is likely to result to individuals if there is a data breach;
- the potential for harm (in terms of reputational or other damage) to the entity holding the personal information; and
- how the entity stores, processes and transmits the personal information (for example, paper-based or electronic records, or by using a third party service provider).

The OAIC suggests that in planning their security safeguards, entities should consider the following steps:

- Risk assessment – Identifying the security risks to personal information held by the organisation and the consequences of a breach of security;
- Privacy impact assessments (or what might be called a partial "privacy audit") – Evaluating, in a systemic way, the degree to which proposed or existing information systems align with good privacy practice and legal obligations;
- Policy development – Developing a policy or range of policies that implement measures, practices and procedures to reduce the identified risks to information security;
- Staff training – Training staff and managers in security and fraud awareness practices and procedures;
- The appointment of a responsible person or position (e.g. a Privacy Officer) – This position could have responsibility for establishing policy and procedures, training staff, coordinating reviews and audits and investigating and responding to breaches;
- Technology – Implementing privacy enhancing technologies to secure personal information, including through such measures as access control, copy protection, intrusion detection, and robust encryption;
- Monitoring and review – Monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures, and ensuring that effective complaint handling procedures are in place;
- Standards – Measuring performance against relevant Australian and international standards as a guide;
- Appropriate contract management – Conducting appropriate due diligence where services (especially data storage services) are contracted, particularly in terms of the IT security policies and practices that the service provider has in place, and then monitoring compliance with these policies through periodic audits.

Another sensible point the OAIC makes is that entities can reduce their data breach risks by ensuring they only keep personal information for as long as necessary (this is required by APP 11.2 in any event). Entities could also consider avoiding the collection of personal information, or certain types of personal information (e.g. credit card numbers), wherever practical.

The following specific ideas for preventing data breaches are given by the OAIC based on its observation of responses in the marketplace to data breaches:

- the creation of a senior position in the agency or organisation with specific responsibility for data security;
- the institution of a ban on bulk transfers of data onto removable media without adequate security protection (such as encryption);
- disabling the download function on computers in use across the organisation, to prevent the download of data onto removable media;
- placing a ban on the removal of unencrypted laptops and other portable devices from the organisation's buildings;

- introducing a policy requiring erasing of hard disk drives and other digital storage media (including digital storage integrated in other devices such as multifunction printers or photocopiers) prior to being disposed of or returned to the equipment lessor;
- the use of secure couriers and appropriate tamper proof packaging when transporting bulk data; and
- the upgrading of passwords (for example, an increase from 6 to 8 characters, including numbers and punctuation), and the institution of a policy requiring passwords to be changed every 8 weeks.

Develop a data breach response plan

The OAIC suggests that an organisation should consider developing a "data breach response plan" as part of its information security strategy under APP 11.1.

The OAIC's Guide to Information Security[14] suggests that the data breach response plan should cover:

- the strategy for assessing and containing breaches;
- the actions that are required under legislation[15] or relevant contracts;
- the key personnel responsible for implementing the strategy (e.g. the Privacy Officer and Chief Technology Officer);
- clear lines of command and accountability for data breach issues;
- a procedure for determining whether to notify affected individuals and/or the OAIC; and
- a strategy for identifying and remediating the source of the data breach to prevent further issues. The OAIC makes the point that it is important to check whether any similar breach has occurred in the past, i.e. whether there is a systemic issue that needs to be addressed. The strategy for preventing further issues might (the OAIC suggests) include conducting
    - a security audit of both physical and technical security;
    - a review of the entity's policies and procedures and making changes to reflect the lessons learned from the investigation, plus regular reviews after that;
    - a review of employee selection and training practices; and
    - a review of service delivery partners (for example, offsite data storage providers).

It would also seem sensible for the data breach response plan to include:

- key contacts from the service providers that handle personal information on behalf of the entity; and
- details of professional services that could be engaged to assist with containing and the data breach and managing the risks it creates (e.g. IT security consultants and legal advisers).

The data breach plan should be drafted to prepare the organisation to handle data breach incidents in a manner that complies with the organisation's legal obligations, addresses the OAIC's expectations (discussed above) and minimises the other potential risks created by a data breach incident (such as financial loss, damage to reputation and legal liability). As such, it would appear sensible for the data breach plan to be integrated into the organisation's broader crisis management/incident response framework.

The OAIC suggests that best practice would involve including information in the organisation's privacy policy about how it will respond to any data breach. However, this information may be of limited value since any response to a data breach will need to be determined (as the OAIC recognises) on a case by case basis. The information in the privacy policy could therefore only be stated at a high level, i.e. "these are the principles and processes the organisation will apply in determining its response to a data breach".

The organisation should consider establishing a "breach response team" that can manage the response to a data breach. The team might include, for example, representatives from the privacy, legal, IT, public relations and senior management areas.

Overseas experience

A number of foreign jurisdictions have introduced varying forms of mandatory data breach notification obligations that apply generally to organisations handling personal information. Some of the important jurisdictions with mandatory notification requirements are discussed below.

Other jurisdictions (such as Japan, Singapore, Canada, Ireland and the United Kingdom) adopt a similar approach to Australia and address data breach notification as part of the organisation's general obligation to keep personal information secure.

The jurisdictions that do have mandatory notification requirements differ in terms of the trigger for notification, the penalties for non-compliance and the risk of civil litigation by affected individuals. The content requirements for the notice are, however, largely similar: a description of the nature of the breach, when and how the breach occurred, a description of the consequences of the breach, and a description of the measures taken or proposed measures taken to address the breach.

United States

The majority of U.S. states have laws requiring notice to be provided to affected individuals in the event of a data breach. U.S. federal and state government entities and

companies in certain industries, such as banking, insurance and health care, are also regulated under specific notification regimes. The trigger for notification can vary – some jurisdictions require notification if there is unauthorised "access", while others only required notification if there is unauthorised "acquisition". Many of the laws require that notice be provided to state and sometimes federal authorities. Government agencies may assess fines and other penalties for non-compliance with notification obligations, but this varies across each U.S. jurisdiction and across industries. Private litigation is also possible, and there has been a rise in class action suits concerning data breaches in recent years. There has been a certain level of dissatisfaction with the mandatory nature of the data breach notification schemes in the U.S. However, given that the U.S. lacks a comprehensive federal privacy/data protection regime it could be argued that there is a greater need for mandatory notification than in other jurisdictions.

European Union

All members of the European Union (EU) are subject to data breach obligations under the European Data Protection Directive (Directive 95/46/EC). Currently, mandatory data breach notification obligations extend only to public electronic communication service (ECS) providers such as Internet service providers and telecommunications providers. However, the draft EU General Data Protection Regulation (set to become law in 2014 and enforceable from 2016 onwards) will see that obligation extended to all companies operating in the EU, as well as to all foreign companies processing data of EU residents. Non-compliance will be subject to fines of up to 2% of the entity's global annual turnover.

South Korea

South Korea's *Personal Information Protection Act 2011* (PIPA) imposes mandatory notification requirements and applies to both the private and public sectors. Under PIPA, notification is only required for data breaches affecting at least 10,000 individuals. In South Korea the affected individual as well as the relevant authority must be notified. Any negligent failure to notify is subject to a fine not exceeding KRW 30 million (about AUD $31,500). Aside from PIPA, data breach notification requirements can also arise under the *Promotion of Information and Communications Network Utilization and Information Protection Act*, which applies to IT service providers and their users. Affected individuals can also bring civil claims for monetary compensation (assessed on a case by case basis).

Conclusion

Although mandatory data breach notification requirements do not currently form part of the Privacy Act regime in Australia, there are still numerous reasons (regulatory and otherwise) for organisations to consider notifying affected individuals, the OAIC and other affected parties in the event of a serious data breach that creates a real risk of harm. Organisations should consider the question of notification in the context of the broader objective of containing the data breach and mitigating the potential risks it creates, and approach the issue in a flexible and case-specific manner.

At the time of writing this paper, the Privacy Commissioner is yet to exercise his new enforcement powers under the Privacy Act 1988 (Cth) in relation to a data breach incident. However, given the increasing frequency and severity of data breach incidents in recent times and the recently strengthened powers of the Privacy Commissioner it appears that such a decision may not be too far away. Organisations should act now to ensure that they have appropriate information security measures in place, including suitable procedures to manage data breach incidents if and when they occur.

---

1 We refer to the Office of the Australian Information Commissioner throughout this paper but note that the recent Federal Budget announced that the Office will be disbanded. The Privacy Commissioner role will remain but a variety of the OAIC's functions will be spread amongst other agencies.

2 Office of the Australian Information Commissioner, *Data Breach Notification - A guide to handling personal information security breaches* (April 2012). Available at http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Data_breach_notification_guide_April2012FINAL.pdf

3 The definition in the Data Breach Notification Guide does not specifically refer to "interference" as the Guide was published in April 2012 and has not been updated to reflect the new language of APP 11 (which introduced the concept of "interference"). For the purposes of this paper we will assume that the definition includes "interference".

4 Office of the Australian Information Commissioner, *Multicard Pty Ltd: Own motion investigation report* (May 2014). Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/multicard-omi.

5 Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own motion investigation report* (March 2014). Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014

6 Office of the Australian Information Commissioner, *Medvet Science Pty Ltd: Own motion investigation report* (July 2014). Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/medvet-science-pty-ltd-own-motion-investigation-report.

7 Office of the Australian Information Commissioner, *Data Breach Notification - A guide to handling personal information security breaches* (April 2012). Available at http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Data_breach_notification_guide_April2012FINAL.pdf

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (12 August 2008. Available at http://www.alrc.gov.au/publications/report-108.

9 Office of the Australian Information Commissioner, *Community Attitudes to Privacy survey Research Report 2013* (9 October 2013). Avilable at http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013#_Toc368300741

[10] Senator Helen Kroger, Chief Government Whip, *Proof Committee Hansard*, Thursday, 19 June 2014, p 14.

[11] See for example, Office of the Australian Information Commissioner, *AAPT and Melbourne IT: Own motion investigation report* (October 2013). Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/aapt-and-melbourne-it-own-motion-investigation-report

[12] Office of the Australian Information Commissioner, *Guide to information security: 'reasonable steps' to protect personal information* (April 2013). Available at http://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

[13] Office of the Australian Information Commissioner, *AAPT and Melbourne IT: Own motion investigation report* (October 2013). Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/aapt-and-melbourne-it-own-motion-investigation-report

[14] Office of the Australian Information Commissioner, *Guide to Information Security* (April 2013). Available at http://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

[15] Mandatory obligations could arise under the laws of other jurisdictions (where the personal information is regulated under the laws of multiple countries), or under specific Australian legislation such as the *Personally Controlled Electronic Health Records Act 2012 (Cth)*.