DATA BREACH NOTIFICATION IN AUSTRALIA

Introduction

The first data breach notification law (DBNL) was introduced in California in 2002 (and enacted in 2003). Since that time, similar laws have been introduced in different forms in nearly all the States in the United States [1] and are under consideration in a number of other jurisdictions. In its most basic form, data breach notification laws require that people be notified if there has been a breach of security in regard to their personal information where held by a third party.

Information about data breaches, at least in the United States, has become much more public. In addition to regular media reporting on data breach disclosures, there are at least two databases where information on data breaches is compiled, one maintained by the Open Security Foundation[2] and the other by Privacy Clearing House.[3] According to the OSF database, the biggest data loss incidents are:

	No. of Records Affected	Date of Breach	Part(ies) Involved
1	150,000,000	2012-03-17	Shanghai Roadway D&B Marketing Services Co. Ltd
2	130,00,000	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
3	94,000,000	2007-01-17	TJX Companies Inc
4	90,000,000	1984-06-01	TRW, Sears Roebuck
5	77,000,000	2011-04-26	Sony Corporation
6	50,000,000	2008-08-27	Unknown Organization
7	40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
8	40,000,000	2011-12-26	Tianya
7	35,000,000	2011-07-28	SK Communications, Nate, Cyworld
9	35,000,000	2011-11-10	Steam (Valve, Inc.)
10	32,000,000	2009-12-14	RockYou Inc

There is no doubt that the wide spread publication of data breach information, as a result of the compulsory notification has greatly increased public interest in data security.

---

1 For a full list of relevant U.S. legislation – see the list published by the National Conference of State Legislation available at http://www.ncsl.org/default.aspx?tabid=13489 Last accessed April 25, 2011.. Also note Kate Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law ' 75 *Fordham L. Rev*. 355 referring to the U.S. position at p361: "In the absence of adequate self-regulation, federal and state governments have stepped in and required businesses to protect their information assets."

[2] http://datalossdb.org/

[3] http://www.privacyrights.org/data-breach

> "Since California enacted the first security breach notification law (SBNL) in 2002, a tidal wave of security breach notices has been unleashed in American consumers, making the problem of inadequate information security in American businesses visible to the public for the first time." [4]

However, it is not absolutely clear that DBNLs are an appropriate response to data security issues. At least one commentator has noted that "it is unclear what, if any, impact, (DBNLs) are having on the total volume of security breaches, or information security more generally."[5] It is worth noting the 6 of the 10 worst data losses according to OSF have occurred in the last 3 years – 5 of those occurring in the last year. Although not conclusive evidence as to the efficacy of data breach notification laws, the large number of significant incidents occurring in 2011 and 2012 indicates that the data breach problem has not been solved. Interestingly, an in depth study released in 2011 on the effect of DBNLs on identity theft (DBNLs being introduced in the U.S. as a specific response to identity theft) indicates a 6% decrease in identity theft in those States where DBNLs have been introduced.[6]

Irrespective of the actual impact the laws are having on the occurrence of data breaches, data breach notification laws (DBNLs) are of interest as one of the most visible regulatory responses identified to deal with a particular information security issue. They are also of interest to information security practitioners in Australia as, if introduced, they will have a huge impact on the current information security landscape. In the meantime, while the legislature continues to consider whether to introduce a DBNL and what form it might take, the Office of the Australian Information Commissioner has recently updated its Data Breach Guidance setting out clearly the OAIC's expectations on "voluntary" notification of data breaches.

In this review of data breach notifications laws, the following will be covered:

- The history and current status of DBNLs in the U.S.
- Privacy legislation in Australia and the proposed inclusion of data breach notification provisions in the *Privacy Act 1988* (Cth)
- The OAIC's Data Breach Notification guidelines
- Corporations Law Disclosure Obligations in Australia
- Disclosure obligations in the *Personally Controlled Electronic Health Record Bill*
- Proposed data breach notification obligations in other jurisdictions –New Zealand, Canada, the EU and the United States.

It will conclude with some recommendations on how Australian organisations should respond to data breaches.

[4] Jane K. Winn 'Are "Better" Security Breach Notification Laws Possible?' 24 Berkeley Tech. L.J. 1133 (2009) at 1133

[5] Jane K Winn "Are "Better Security Breach Notification Laws Possible?" p1133

[6] Romanosky, Telang and Acquisti in the original paper "Do Data Breach Disclosure Laws Reduce Identity Theft" released in 2008 and updated and re-released in 2011.

DATA BREACH NOTIFCATIONS LAWS IN THE UNITED STATES

As already noted, data breach notification laws were first introduced by the state of California in 2002.

Most commentators give two reasons for the passage of DBNLs:

- to inform consumers when unauthorized individuals have accessed their personal information so they can take precautions to prevent or minimize harm, and
- to encourage businesses to improve data security to prevent breaches that will trigger consumer notification.[7]

Since that time, some 45 states in the United States have introduced either the same of some variation of the Californian DBNL.

Types of DBNL

Trigger: Different regimes exist in different States – with different triggers for notification. Twenty five state laws require notification when the personal information is reasonably assumed to have been acquired by an unauthorized party (called the "unauthorised acquisition test"). This is what was used in the Californian provision, which requires notification where any owner of a system discovers or is notified of "a breach in the security of the data of any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.

Other state laws require notification only if it is reasonable to believe the information will cause harm to consumers.[8] This is called the "harm" trigger and has been criticised as allowing the breached organisation too much discretion to determine whether or not to give notice. Some States limit the harm to a reasonable belief that the breach has or will cause identity theft to any consumer (Kansas) or to a breach which poses a significant threat of identity theft (Rhode Island).

Some jurisdictions impose additional hurdles – requiring the likelihood that the material will be misused or that the breach be material.[9]

Encryption Exemption: The Californian DBNL does not apply to lost data that was encrypted, and most States exclude encrypted or password protected data, providing the encryption key has not also been stolen.

Timing: The Californian requirement is for notice to be given "in the most expedient time possible and without reasonable delay consistent with the legitimate needs of law enforcement ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

Jurisdiction: Some laws apply depending on the residency of the consumer while other rely on the location of the breach. Georgia's law only applies to information brokers and data collectors – while

[7] See e.g. Paul Schwarz and Edward Janger 'Notification of Data Security Breaches" (2007) 105 Mich. L. Rev 913, Kathryn E. Picanso 'Protecting Information Security Under a Uniform Data Breach Notification Law' 75 Fordham L. Rev. 355 and Jennifer Chandler 'Negligence Liability for Breaches of Data Security' Banking & Finance Law Review (Feb 2008); 23, 2, 223 at 224 - 225

[8] Romanosky et al 2011 at 4 and Mark Burdon at 124

[9] E.g. Florida, Arkansas and Wisconsin

the law in Oklahoma applies to "any state agency, board, commission or other unit ... of state government that owns or licenses computerized data that includes personal information."

Definition of "Personal Information": There are different definitions of "personal information" – some quite prescriptive but others more general, referring to any information that could be used to support identity fraud. The Californian provision refers to an individual's first name or first initial, last name, and at least a social security number, driver's license number or state identification card number, or an account number, credit card number or debit card number in combination with any security code necessary to access a financial account.

Computerized Records: The Californian and most other DBNLs only apply to computerised data, which means that paper records fall outside the law of most States.

Form of Notice: Different states have different requirements regarding the content of the notice, and how it should be served. California has recently introduced a new online form and requires businesses to submit the electronic reporting form and upload a sample copy of the notification letter being sent to affected individuals when a breach affects more than 500 Californian residents.

Criticisms of DBNLs

One of the major criticisms of DBNLs is the "stand alone" nature of the requirement. DBNLs are modelled on "community right to know clauses" which were developed to improve the efficacy of environmental laws. In this case – there is no other regulation, no mandatory minimum levels of computer security or statutory right to damages for breach of privacy – so the DBNLs operate in isolation and do not provide a "coherent regulatory framework". [10]

Other issues include:

- DBNLs place "strict liability" on the notice issuer who has to comply even where not negligent. "SBNLs establish an inequitable strict liability regime because when breaches occur they do not distinguish between companies that implement information security best practices and those that show a reckless disregard for the security of sensitive data."[11]
- DBNLs do not change the position in regard to the manufacture of products without appropriate security
- The causal link between data breach and identity theft has been questioned (which raises a question mark regarding the policy imperatives supporting the introduction of DBNLs).[12]
- Notification fatigue - When the Choicepoint datamining company was breached in 2004 the company offered credit protection and monitoring services to those whose information had been compromised. Fewer than 10% of the 163,000 consumers availed themselves of free credit monitoring services following the Choicepoint breach (Brodkin 2007).[13] An FTC Study in 2007 found that 44% of identity theft victims ignored breach notification letters. A Ponemon 2008 survey found that 77% of respondents claimed to be concerned or very concerned about loss or theft of personal information – but only 47% took advantage of free

[10] Jane K Winn p1135
[11] Jane Winn at 1159
[12] Mark Burdon "The mandatory notification of data breaches: Issues arising for Australian and EU Legal Developments"p126. Also Romanosky 2010 "... if the vast majority of identity theft does not originate from data breaches (ether because the information is simply lost and will never be used maliciously, or because credit card companies reimburse consumers for their loss) then the maximum effectiveness of these laws may inherently be limited."
[13] "Do Breach Notification Laws Work?"By Kim Zetter March 9, 2009 http://www.wired.com/threatlevel/2009/03/experts-debate/# Accessed February 17, 2011

or subsidised credit monitoring services.[14] As notifications have become more ubiquitous — 55 percent of respondents in a 2008 Ponemon Survey said they'd received two or more notices within 24 months — many consumers have become inured to them, simply tossing them in the trash rather than acting on them to protect their identity.[15]

- Encryption safe harbor provisions: Many of the DBNLs provide a safe harbor for companies who encrypted data. The specific wordings of the provisions vary between States but there are questions as to the efficacy of the provisions. [16]

Notwithstanding these criticisms, DBNLs have been generally supported and their introduction has been recommended in most jurisdictions. However, to date there has not been the same adoption of broader information security laws such as those introduced in California to regulate information security practices[17] by State legislatures across the United States.

PRIVACY LEGISLATION IN AUSTRALIA

There are currently no legislated mandatory data breach notification requirements in Australia. However, the inclusion of a requirement for notification of data breaches as part of the Privacy Act provisions has been under consideration for some time[18] and there is growing pressure from various sources for it to be introduced.

Both the previous and the current Privacy Commissioners have supported the introduction of mandatory data breach notification.[19] The Office of the Privacy Commissioner (OPC) supported the introduction of DBNLs in its submissions to the ALRC. That support was more recently confirmed in submissions made by the Office of the Australian Information Commissioner (OAIC) of which the OPC now forms part, to the Department of Prime Minister and Cabinet in response to the Cyber White Paper discussions,[20] which again raised the question of how the reporting of data breaches should be handled and encouraged.

In April 2012, on the release of the new *Data Breach Notification* guide,[21] replacing the August 2008 *Guide to handling personal information security breaches*, the Australian Information Commissioner noted that, though there had been little movement on the issue, there was "strong support for the notion that the Government must treat data breach notification as a mandatory process". He also noted that that "internationally, the tide is moving in this direction"[22] referring to the European Union, the United States and the United Kingdom and further noted that "The Australian

[14] Romanosky et al 2011
[15] Zetter article n123.
[16] Burdon, Mark; Reid, Jason et al "Encryption safe harbours and data breach notification laws" Computer Law & Security Review 26(5): 520 – 534
[17] See California Civil Code Section 1798.81.5 which requires businesses that own or license personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
[18] Inclusion of a mandatory data breach notification provision was recommended by the Australian Law Reform Commission in its 2008 report. This is discussed later.
[19] See for example Dearne K 'Data in danger' *The Australian* (IT news section) 1 May 2007 and Office of the Privacy Commissioner media release 'Privacy Commissioner calls for mandatory reporting of major data security breaches' (30 January 2008).
[20] http://cyberwhitepaper.dpmc.gov.au/published-submissions
[21] http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html
[22] http://www.oaic.gov.au/news/speeches/john_mcmillan/john_mcmillan_120430_paw.html

government is aware of those developments and I expect the data breach notification framework will continue to be considered." [23]

A survey released in April 2012 shows that 80% of those surveyed supported the introduction of mandatory data breach notification laws.[24] In responding to that report, the Australian Privacy Commissioner said the results were "not surprising" given that "(o)ver the last 12 months the community has seen a number of very significant data breaches" attributable to the increasing exposure of weaknesses in business systems coupled with more sophisticated online hackers. [25]

Influential information security organisations have come out in favour of data breach notification laws, one well known vendor recently referring to Australia's failure to pass DBNLs being a regional disappointment given Australia's leadership role in setting standards in other areas, such as financial regulation.[26]

However, support for DBNLs is not unanimous. In their submissions as part of the Cyber White Paper discussions, Optus and Telstra were of the view that the OAIC's voluntary data breach notification guidelines would be sufficient, although Telstra also thought that legislation to support such reporting should be examined. The Internet Industry Association (IIA) took a similar view, but reasoned that establishing laws to force breach notification could be at the detriment to local industries.[27] Electronic Frontiers Australia was reported at the time as taking a neutral stance but has since come out publicly in favour of mandatory data breach notification.[28]

Similarly, the Attorney-General's Department, while acknowledging that the topic of data breach notifications was previously recommended as an issue raised by the Quintet of Attorneys-General, did not explicitly list it as a priority area that the Cyber White Paper should consider.[29]

Perhaps not surprisingly it is still not clear if or when data breach notification laws will be introduced in Australia. However, there are voluntary reporting expectations which have recently been strengthened and which reflect in most way the 2008 ALRC recommendations.

It is still prudent for organisations to understand both the current obligations under the Privacy Act and the Privacy Commissioner's expectations in regard to data breaches in the context of the ALRC recommendations.

Privacy Act 1988 (Cth)

The Privacy Act 1988 (Cth) regulates "information privacy", which is taken to mean the protection of personal information for the purposes of the Act. It applies to all federal government department and agencies and (since 2001) to all private sector organisations, other than "small businesses". [30]

[23] http://www.computerworld.com.au/article/423099/oaic_updates_data_breach_guidelines/
[24] http://www.canberra.edu.au/cis/thoughtleadership/research-papers/
[25] http://www.canberra.edu.au/media-centre/2012/may/australians-demand-online-data-breach-notification-uc-survey-reveals
[26] http://www.zdnet.com.au/oz-left-behind-on-data-breach-laws-verizon-339324996.htm
[27] http://www.zdnet.com.au/australia-divided-over-data-breach-laws-339332126.htm
[28] http://www.itwire.com/it-policy-news/regulation/54618-efa-demands-data-breach-disclosures
[29] http://www.itwire.com/it-policy-news/regulation/54618-efa-demands-data-breach-disclosures

The Act contains a set of principles[31] which are the base line privacy standards for those sector organisations to which the Act applies. These Principles include a requirement for each private sector organisation covered by the Act, to "take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure."[32] The Act specifically provides that organisations covered by the Act shall not breach a privacy principle[33] although currently the enforcement options available to the OPC in the case of breach are somewhat limited.

The operation of the Privacy Act was extensively reviewed by the Australian Law Reform Commission (ALRC) which included consideration of the inclusion of data breach notification provisions.

ALRC Recommendations

As part of the 295 recommendations made in its final report, "For your information: Australian Privacy Law and Practice"[34] tabled in August 2008, the ALRC recommended that the Privacy Act be amended to require notification of data breaches in certain circumstances. The ALRC notes that there were a number of submissions made on the question of DBN however there was not unanimous support for its introduction.[35]

The most contentious issue was the trigger for notification.

Following its consideration of the various submissions and after referring to existing DBN requirements in other jurisdictions, the ALRC recommended that an organisation would need to notify affected individuals and the Privacy Commissioner if:

- there has been unauthorised access to certain "specified personal information" (which will be defined to include information, such as financial information, that is most likely to cause harm to an individual if compromised); and

- the unauthorised access may give rise to a **real risk of serious harm** to any affected individual.

---

[30] Small businesses are those with an annual turnover of $3 million or less or any size business of a particular type e.g. a health service provider, a business that trades in personal information or whichi s related to a larger business.

[31] National Privacy Principles (NPPs) for private sector organisations and Information Privacy Principles (IPPs) for the public sector.

[32] National Privacy Principle 4 (NPP 4) is applicable to private organisations. The wording of Information Privacy Principle 4 (IPP 4) which applies to government bodies, is slightly different providing "A record-keeper who has possession or control of a record that contains personal information shall ensure... that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse." The difference is that agencies are obliged to take steps to prevent the unauthorised use or disclosure of personal information that has been disclosed to a third party in connection with the provision of a service to the agency. No equivalent obligation applies to organizations. NPP 4 is available for download at http://www.privacy.gov.au/materials/types/infosheets/view/6583#npp4. IPP 4 is available for download at http://www.privacy.gov.au/materials/types/infosheets/view/6541#d.

[33] Section 16 Privacy Act

[34] http://www.alrc.gov.au/publications/report-108

[35] ALRC Report 108 Section 51.48 at p1681

It was also recommended that failure to notify the Privacy Commissioner of a relevant data breach would be a civil penalty offence.

The rationale for introducing data breach notification included:

- Concerns about identify theft and identity fraud. Notification would give affected person the opportunity to take protective measures.
- Lack of market incentives for notification
- Incentives to secure data (given the reputational damage that can flow from having to disclose a security breach)
- Increasing number of data breaches[36]

"Specified Personal Information"

Since the release of the report, there has been little consideration of what the limitation of the DBNL to "specified personal information" might mean. At the time it was clearly intended as a way of limiting disclosure to the identity theft type cases which were the policy basis for the introduction of the requirements. This linkage however has disappeared in the voluntary guides published by the OPC which include a consideration of the sensitivity of the information as part of the decision as to the level of risk of serious harm.

The latest Data Breach Notification Guide, by placing notification within the context of taking reasonable security measures as required by the Privacy Principles, further distances the Australian DBNLs from the link to identity theft which still provides the context for most of the DBNLs in the United States.

"Real Risk of Serious Harm"

The "real risk of serious harm" threshold is intended to reduce the compliance burden on organisations and also to reduce the possibility of "notification fatigue" where individuals receive so many notices that it becomes difficult for them to distinguish the security breaches that carry a real risk of harm from those that are minor in nature and consequence.

The ALRC recommendations indicated that a number of factors should be taken into account when assessing whether there is a risk of serious harm from a security breach, including whether the compromised information was adequately encrypted. Again, it is clear from this that the ALRC does not intend notification requirements to apply where, despite a breach in security, there is little prospect that compromised information will be used for unauthorised purposes.

The Government intends to address the ALRC's mandatory data breach notification recommendation in the second tranche of privacy reforms, which as at the date of this paper have still not been released. Until that time, the Office will continue to monitor the operation of the voluntary Guide and assess strengths and weaknesses that may have a bearing on the future development of legal provisions.

Voluntary Data Breach Notification Guide

Although there is still no indication of when a mandatory data breach notification law might be considered, in August 2008 the Privacy Commissioner released a voluntary guide to handling security breaches, which includes consideration of notification as part of the breach response.

[36] ALRC Report 108 Section 51.4 – 51.13 at pp1168 - 1671

The 2008 Guide was released following an open consultation on a draft version during which the Office received 75 submissions from stakeholders. It followed the release of similar guides in Canada and New Zealand – and borrows heavily from those documents. The 2012 Guide, which supersedes the 2008 Guide, was released as part of Privacy Awareness Week.

The new Guide sets out what the Office believes are the key steps and factors for agencies and organisations to consider when responding to a personal information security breach. This includes when it may be appropriate to notify individuals (and in some cases the Privacy Commissioner) of a breach without the sole focus being notification of breaches. The guide encourages a risk-analysis approach so that agencies and organisations evaluate a breach on a case-by-case basis and make decisions on actions to take according to their own assessment of risks and responsibilities in their particular circumstances. The guide also highlights the importance of preventative measures as part of a holistic information security plan.

While compliance with the guide is voluntary, it represents current best practice and may be used as a reference point for government when formulating any new mandatory notification laws. In relation specifically to breach notification, the Guide recommends it as good privacy practice for the reasons that:

- Notification as a reasonable security safeguard (as required by NPP4 and IPP4)
- Notification as openness about privacy practices, which is recognised as a fundamental privacy principle.
- Notification as restoring control over personal information
- Notification as a means of re-building public trust

The Guide follows a four step approach in responding to data breaches (with notification being part of Step 3):

Step 1: Contain the breach and do a preliminary assessment

Step 2: Evaluate the risks associated with the breach

Step 3: Consider notification

Step 4: Prevent future breaches

As part of the risk evaluation to be done in Step 2, the Guide recommends consideration of the following factors:

- What personal information is involved
- What is the context of the information
- The cause and extent of the breach
- The risk of harm that could result to individuals
- Other harms or risks that could arise

The Guide states that those affected should be notified if there is a real risk of serious harm, which is the same trigger threshold as recommended by the ALRC.

According to the Guide, factors to be considered when deciding if notification is required (assuming there is a real risk of serious harm) include:

- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach?
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised very sensitive or likely to cause humiliation or embarrassment for the individual?
- What are the legal and contractual obligations to notify and what are the consequences, of notification?
- What are the consequences of failing to notify affected individuals? If individuals subsequently find out about the breach through the media for example, what could be the associated loss of trust that the agency or organisation sustains?

Consideration on what should be included in any notification and who should be notified is also covered.

Other inclusions in the 2012 Guide are:
Reasonable Security: The Guide repeats at length some of the Guidance contained in other documents as to what are reasonable security measures in the introductory section on "Considerations for Keeping Software Secure." It also incorporates two key privacy principles into the ambit of security – namely the principles limiting the collection of personal information to that which is necessary and requiring the destruction of information once it is no longer required.
Tips for Preventing Future Breaches: Some suggestions are made for simple controls that can assist.
Reporting a Data Breach of the OAIC: This provides information not only on what the OAIC can and can't do when notified but also includes contact details and the information that should be included in the notice to the OAIC.
Data Breach Response Process: An easy to follow flow chart of the process is included at the end of the Guide.

While the Guide is useful, it still leaves significant grey areas. For example, there is no definitive ruling on when a breach will give rise to a risk of serious harm. The 2012 Guide includes some useful examples of how the steps might work and how the risk assessment might apply. However, an organisation will always need to exercise some subjective judgement when considering whether a notification is necessary or appropriate.

In addition, there is no clear guidance as to the required timing of any breach notification — the Privacy Commissioner has simply indicated that notification should take place "as soon as reasonably possible" after the breach. There would be little gain from forcing organisations to issue immediate notifications that do not contain full or accurate details of the breach, as incomplete notifications may be misleading and could spark unnecessary concerns amongst users.

Finally, there is no power for the Privacy Commissioner to audit compliance with the Guide. However, complaints regarding non-compliance could be brought on the basis of breach of NPP4 – as a failure to take reasonable security measures.

Practical Experience

According to the Office of the Australian Information Commissioner, since the introduction of the original guide tin 2008 the Office has received data breach notifications from private sector organisations and from government agencies. As well, the Office has received positive feedback from business and government on the Guide with one agency using the Office's Guide reporting that they received positive feedback from a client about how they dealt with a data breach.[37]

[37] See the 2011 Annual Report at http://www.oaic.gov.au/publications/reports/annual-report_10-11/chapter5.html

Again according to the OAIC, the nature of DBNs mean that the OAICs investigation of these incidents primarily focuses on the data security measures agencies and organisations had in place when the incident occurred and the steps taken to improve such practices as a result of a DBN. The OAIC has said it will look at each DBN "to assess if further action is required by the agency or organisation to appropriately respond to the breach." In particular it will be interested to ensure that the organisation has contained the breach by recovering the information or has taken steps that mitigate further impact on individuals affected by the breach, such as notifying relevant authorities and individuals and taking steps to review and improve data security practices. If the Office feels that inadequate steps have been taken or the agency or organisation is still assessing the source and impact of the breach and the overall response that is required, it will work with the entity to assist it to apply best privacy practice. In cases where the OAIC is not satisfied with the voluntary action taken by the agency or organisation to resolve the matter, it will open an OMI.[38]

In the 2012 Guide, the OAIC makes it clear that, although mandatory data breach notification is not required, it does expect to be notified if there is a real risk of serious harm or if there is any doubt as to whether or not that threshold might be met. While providing detail on the various benefits of notifying the OAIC, the Guide also refers to the available powers in the case of unreported breaches – including the ability of the Privacy Commissioner to instigate own motion investigations (and publish the results) as well as to make determinations requiring the payment of compensation for damages or other remedies, such as the provision of access or the issue of an apology.

Following the release of the original guide in 2008, there were 44 instances of voluntary reporting of data breaches in the 2009 -2010 year, increasing to 56 in the 2011 reporting period.[39]

Incidents reported to the OAIC through DBNs in 2010–11 include:

- documents containing personal information were faxed to the wrong fax number
- an email containing personal information was sent to a public email address
- a system error occurred allowing customers to access other customers' accounts
- a computer containing customer records was stolen from a company's premises.[40]

Typically, the actions taken by entities in response to a DBN include system reviews and alterations, written notifications to affected individuals, apologies, retrieval of records, changes in standard operating procedures and staff training.

Conclusion

Traditionally, the Office of the Privacy Commissioner has exercised its investigatory and settlement powers the Privacy Act in a conciliatory manner, and the Privacy Commissioner has come under attack for taking this approach to dealing with infringing conduct. The Office has been criticised for being reluctant to exercise its powers and not being sufficiently proactive. However, that approach is set to change. In a recent speech, the Commissioner vowed that:

> For particularly serious privacy breaches, or where conciliation is not appropriate, I am prepared to use my power to make determinations directing how complaints should be resolved. My determinations are enforceable in the Federal Court.[41]

---

[38] Chapter 5 2011 Annual Report

[39] Taken from The Office of the Australian Information Commissioner, Australian Government "Annual Report 2010 – 2011" (2011 Annual Report) and the Office of the Privacy Commissioner, Australian Government "Operation of the Privacy Act Annual Report 1 July 2009 -30 June 2010" (2010 Annual Report)

[40] Chapter 5 2011 Annual Report

41M Lee, 'Privacy Commissioner to hit leakers hard', http://www.zdnet.com.au/privacy-commissioner-to-hit-leakers-harder-339327067.htm.

Given this attitude, it is prudent for all organisations to be aware of the current state of play of data breach notification in Australia and to start preparing themselves for a more active Privacy Commissioner committed to undertaking more Own Motion Investigations and to making more Determinations in cases of data breach – whether or not data breach notification is made a legislative requirement pursuant to the Privacy Act.

Privacy Law in Other Jurisdictions

When releasing the new Data Breach Notification Guide, the Information Commissioner referred to the international trends towards the introduction of mandatory data breach notification. It is worth reviewing the current status of data breach notification laws in some of the more relevant jurisdictions.

New Zealand

The Privacy Act 1993[42] controls how "agencies" collect, use, disclose, store and give access to "personal information" in New Zealand. Almost every person or organisation that holds personal information is an "agency". So, for example, the Privacy Act covers government departments, companies of all sizes, religious groups, schools and clubs.[43] At the heart of the Privacy Act are twelve privacy principles, similar to those included in the Australian Privacy Act. The privacy principles cover the collection, access and correction, accuracy and use and disclosure of personal information. Principle 5 covers the storage and security of personal information – and requires that information be protected by "such security safeguards as it is reasonable in the circumstances to take."[44]

In July 2011 the New Zealand Law Commission completed a privacy review that began in 2006, with a report "Review of the Privacy Act 1993" (Report) released in August 2011. The overall recommendation in the Report is that the Privacy Act should be replaced by a new Act, implementing the recommendations in the Report and in the Privacy Commissioner's *Necessary and Desirable: Privacy Act 1993 Review*, initially published in 1998 (New Act). In addition, recommendations were made in regard to adding to the Privacy Commissioner's power, making the requirement to undertake Privacy Impact Assessments more explicit and in relation to introducing a mandatory data breach notification requirement.

The report notes that that there was a fairly even split in submissions on whether there should be a mandatory data breach notification provision.[45] Criticisms included:

- Lack of evidence supporting the idea that data breach notification reduced identity fraud
- The notification burden on businesses
- The penalisation of "good players" i.e. those who know that they have had a breach[46]

Given the criticisms, the Law Commission steers clear of recommending an absolute data notification requirement, recommending that notification only be required in certain confined circumstances. [47] Two criteria for mandatory notification are recommended:

- where notification may allow the individual to mitigate a significant risk of real harm to the individual; or
- where the breach is serious, with seriousness being assessed having regard to matters such as the importance or sensitivity of the information, the scale of the breach (whether it affects a small group or a large number of people) or where it is reasonably foreseeable that significant harm might result.[48]

---

[42] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html
[43] http://privacy.org.nz/the-privacy-act-and-codes/
[44] http://privacy.org.nz/storage-and-security-of-personal-information-principle-five/
[45] Law Commission Report Chapter 7 at Section 7.15 p208
[46] Law Commission Report Chapter 7 at 7.16
[47] Recommendation R67 Law Commission Report Chapter 7 at p211
Ezine Simpson Grierson **'The Law Commission's Report on the Privacy Act - a new Act?'** 19 December 2011
[48] Recommendations R68, 69 and 70 Law Commission Report Chapter 7 at p212

It is recommended that notification be given to both the Privacy Commissioner and the individual(s) concerned. However, it is also recommended that the Privacy Commissioner should not publish the identity of the breaching agency unless the public interest so requires (and, where an agency appropriately mitigates the effects of the breach and otherwise acts responsibly, it may be that there is no public interest in "naming and shaming" the business).[49]

Notification should be made as soon as reasonably practicable and in a form such as to fully and fairly inform the individual and where practicable steps he may take to mitigate his loss.[50]

Other recommendations include:

- The Commissioner should have the power to issue a Compliance notice in the case of failure to comply;[51]
- From a legislative perspective, the requirement should be included as part of Principle 5 (the data security principle);[52]
- The Commissioner should publish Guidance about the requirement.[53]

Like Australia, until the review recommendations are made into law, there are only voluntary guidelines for responding to breaches in New Zealand.

The New Zealand Privacy Commissioner introduced a set of "voluntary" guidelines in late 2007, before the Australian guidelines were issued and which were closely modelled on similar guidelines issued by the Canadian Privacy Commissioner (on 1 August 2007). They are largely similar to the 2008 Australian guidelines (which used the New Zealand guidelines as reference).

Canada

The main legislation covering privacy in Canada is the *Personal Information Protection and Electronic Documents Act* (PIPEDA) which applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of its commercial activities, although there are some significant exceptions. The PIPEDA requires organizations to comply with a set of legal obligations that are based on ten principles similar to the National Privacy Principles included in the Australian Privacy Act,

The PIPEDA does not currently contain data breach notification provisions. The Commissioner has asked that PIPEDA be amended to include a mandatory requirement for breach notification and in the meantime, has developed Breach Notification Guidelines to help guide organizations in deciding when to notify, whether to notify, who should be notified, how and under what circumstances.

In 2007, the Commissioner released its guide "Key Steps for Organizations in Responding to Privacy Breaches",[54] which has been widely used by other privacy regulators, including the Australian and New Zealand Privacy Commissioners.

[49] Recommendations R71 and R72 Law Commission Report Chapter 7 at p213
[50] Recommendations R73 and R74 Law Commission Report Chapter 7 at p213 - 214
[51] Recommendation R77 Law Commission Report Chapter 7 at p468
[52] Recommendation R78 Law Commission Report Chapter 7 at p468
[53] Recommendation R79 Law Commission Report Chapter 7 at p468

[54] http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm

European Union

Currently, EU law only requires Member States to enact laws creating a breach notification obligation for telecommunications operators (which some Member States have yet to enact), although some Member States (such as Austria and Germany) do have security breach notification requirements for data controllers other than telecom operators.

In late January 2012, the European Commission released its proposal for a comprehensive reform of the EU's 1995 data protection rules. [55] Proposed changes to the EU Data Protection Directive include the introduction of a breach notification mandate that will apply to all organisations that hold personal information. Pursuant to the proposed reform, in the event of a serious breach, organizations must notify the national supervisory authority "as soon as possible (if feasible within 24 hours)." The trigger for notification to individuals (rather than data protection authorities) is when the breach "is likely to adversely affect the protection of the personal data or privacy" of the individual.

Notification to data subjects is not required if "the controller has demonstrated to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measure, and that those measures were applied to the data concerned by the personal data breach."

The Commission's proposals are in draft and are to be passed on to the European Parliament and EU Member States (meeting in the Council of Ministers) for discussion. If approved, the Regulation will be enforceable in all Member States two years after it has been adopted. Member States will also have a period of two years to transpose the provisions in the Directive into national law. It is currently thought that the amendments will be passed in 2014 or 2015.

Federal United States Data Breach Notification Law

As already discussed, most states in the US have passed their own data breach notification laws, many based on the Californian law that requires notification of security breaches to affected consumers residing in California. However, there are a number of different proposals currently being considered by the US legislature to create a consistent national notification scheme. The model proposed by the Obama administration would only apply to businesses that collect "sensitive personally identifiable information" concerning more than 10,000 individuals during any 12 month period. These businesses would be required to notify affected individuals of a data security breach unless there is no reasonable risk that the breach will result in any harm. Notifications would need to be made without unreasonable delay and no later than 60 days from the breach. Other proposals currently being considered might require faster notification, with one suggestion being that the notification should take place within 48 hours of completing an investigation into the breach. It remains to be seen which approach the US legislature will prefer.

[55] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm. For more information on the EU Data Directive Legislation & Cases: http://ec.europa.eu/justice/data-protection/law/index_en.htm. For more information on the proposed amendments, refer to the Data Protection Reform Mini Site: http://ec.europa.eu/justice/data-protection/minisite/index.html or the Data Protection Reform FAQ: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=fr

Corporations Act and ASX Listing Rules Disclosure Obligations

As well as the proposed provisions to be included in the Privacy Act, it could be argued that there are currently other statutory disclosure requirements that apply to data breaches. An example is the existing continuous disclosure obligations affecting listed companies.[56]

Pursuant to the Corporations Act[57] and the ASX Listing Rules, listed companies must disclose information that is not generally available and that might reasonably be expected to have a material effect on the share price of the entity, and which information the entity becomes aware of.
For the disclosure obligation to apply, three conditions need to be satisfied:

- There must be **information**: Although this is not defined examples are given e.g. a change in the company's financial forecast or expectation or giving or receiving a notice of intention to make a takeover
- The Company must be **aware** of the information
- The information might reasonably be expected to have a **Material effect** on the price or value. There is a test for material.[58]

Impact on share price depends on type and extent of breach and nature of business. The Impact on the share price for Choicepoint (whose business was the supply of confidential information) was dramatic – it went out of business. Conversely, the Sony share price seems to be unaffected by the recent significant data breaches. Similarly, there is research that indicates that the share price impact may be temporary – though may be more damaging for more visible corporations.[59]

K M Gatzlaff and K McCullough, found that:

- The overall effect of a data breach on shareholder wealth is negative and statistically significant.
- There is a negative association between market reaction and firms that are less forthcoming about the details of the breach.
- Firms with higher market-to-book ratios experience greater negative abnormal returns associated with a data breach.
- Firm size and subsidiary status mitigate the negative effect of a data breach on the firm's stock price
- The negative market reaction to a data breach is more significant in the most recent time periods of the sample.[60]

Other research has found that one in 10 large UK businesses has experienced a data leak, and 91 per cent of these suffered reputational damage as a result. The same research also found that 27 per cent of businesses lost their competitive edge as a result of these leaks.[61]

---

[56] For a comprehensive analysis of existing breach notifications laws in Australia, refer to Low, R., M. Burdon, and P. von Nessen, Notification of data breaches under the continuous disclosure regime. Australian Journal of Corporate Law, 2010. 25(2): p. 70ï 100
http://eprints.qut.edu.au/38444/1/LOW_-_Published-Aust_Jnl_of_Corp_Law_v25%2C_n1%2C_pp70-100_2011.pdf

[57] Corporations Act Section 674(2)

[58] Corporations Act Section 677

[59] A Acquisti, A Friedman and R Telang "Is there a cost to Privacy Breaches? An Event Study" Paper presented at the 27th Conference on Information Systems, Milwaukee USA 2006

[60] K M Gatzlaff and K McCullough "The Effect of Data Breaches on Shareholder Wealth" (2010) 13(1) Risk Management and Insurance Review 61

[61] Report: http://www.computing.co.uk/ctg/news/2035786/report-breach-cost-increases-cent-gbp19m Last accessed 31/10/2011

Listed companies who are the victims of a significant data breach should at least consider whether they have any disclosure obligation pursuant to the Corporations Act. Particularly given that continuous disclosure and misleading conduct are once again in the spotlight following the Australian Securities and Investment Commission's successful legal action against Fortescue Metals Group and its CEO, Andrew Forrest.

It is also relevant to note that on October 13, 2010 the SEC in the U.S. issued a Disclosure Guidance that advises public companies on the need to disclose their material cybersecurity risks (as part of their general duty to disclose material information to investors).[62]

Risk assessment is necessary to make the determination on whether disclosure is called for. The Guidance indicates that public companies are expected "to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents." This evaluation will include consideration of the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. The impact of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware is relevant to this evaluation.
If an organisation determines that disclosure is required, the registrant is expected to "describe the nature of the material risks and specify how each risk affects the registrant," avoiding generic disclosures. More specifically, the Guidance states that appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

This Guidance is likely to lead to public companies in the U.S. performing formal and detailed assessments of the cybersecurity risks, and may lead to shareholder litigation following data security breaches with claims that a company failed to perform the assessment and disclose the risks recommended in the Guidance for compliance with securities disclosure laws.

The SEC guidance also underlines the importance of process and risk assessment.

The SEC Guidance – although only binding on U.S. listed companies – may well be relevant to compliance with the Australian legislation and issues of materiality for Australian companies.

Some of the other Corporations Act obligations which may be relevant include:

- Directors' ***duty to make full and frank disclosure*** of information within their knowledge to enable shareholders to make properly informed judgments on any matter [63]

[62] SEC Division of Corporate Finance Disclosure Guidance 2 Cybersecurity:
http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[63] Corporations Act section 191

- Obligation not to make false or misleading statements.[64]

Effective management of breach notifications

To meet customer expectations and those of the Privacy Commissioner, even under the voluntary notification regime, organisations should ensure that they have strong and reliable processes in place to first identify and assess the potential impact of any security breach and then any notifications that may be required. These processes should include:

- a requirement that any actual or suspected data security breach be reported to the organisation's designated privacy officer. The initial report should include as much information as possible about the breach, including the nature of the information in question and the number of affected individuals;
- if notified of a breach, the privacy officer should make an initial assessment as to whether the breach is reasonably likely to cause serious harm to any affected individual. If in doubt – it may be appropriate at this stage to also seek legal advice. Reference should be made to the published Guidelines when making this assessment. Matters to be considered include:
    - What personal information is involved
    - What is the context of the information
    - The cause and extent of the breach
    - The risk of harm that could result to individuals
    - Other harms or risks that could arise

Once an initial assessment has been formed, a legal opinion on the assessment should be sought and documented.

If a breach is assessed as potentially serious, then notification may be required.

The Commissioner's Guidance lists factors to be considered when deciding if notification is required (assuming there is a real risk of serious harm) which include:

- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach?
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised very sensitive or likely to cause humiliation or embarrassment for the individual?
- What are the legal and contractual obligations to notify and what are the consequences, of notification?
- What are the consequences of failing to notify affected individuals? If individuals subsequently find out about the breach through the media for example, what could be the associated loss of trust that the agency or organisation sustains?

All relevant stakeholders should be included in the determination of the appropriate response.

Those stakeholders to be included in the decision making should be specified in the security incident response procedure. At a minimum, consideration should be given to including the following stakeholders: the privacy officer; a legal representative; a manager from the part of the business affected by the breach; and a representative from the organisation's public relations group.
As soon as possible after doing a preliminary investigation (to understand the nature and extent of the breach) and making decisions as to the containment of the breach (if possible and to the extent desirable at the time), the stakeholders should determine whether third parties such as regulators and affected individuals should be notified of the breach. The more definite information that is available about the cause and extent of the breach the better in terms of being able to provide accurate information to external parties.

[64] Corporations Act section 1041e

If the stakeholders determine that a notification is not required, or can be delayed, they should ensure that their reasons for reaching this conclusion are recorded and defensible. In particular, they should have good grounds for concluding that serious harm is unlikely to flow from the breach (eg that the information was adequately encrypted or that any compromised information cannot be connected with any individual).

If in doubt about whether notification is necessary, the stakeholders should consult with the Privacy Commissioner. If the Commissioner advises notification is necessary, they may also be able to provide further guidance on what the format and content of the notification should be. Apart from this practical assistance, involving the Commissioner at an early stage may also enhance the public's confidence in the organisation. Additionally, if the Commissioner advises against notification yet the breach becomes public, the organisation can point to its reliance on the Commissioner's advice as a method of rebutting any resultant criticism and mitigating any reputational harm.

Above all, organisations should remember that they will be judged not only by the level of security that they apply to the information that they possess but also on how they react when that security is compromised. An organisation could suffer an irreversible loss of confidence if it is seen to be concealing a serious breach. By contrast, a proactive, positive and open response to a breach is much more likely to preserve the organisation's reputation and also ensure ongoing compliance with legal notification requirements.

PCEHR LEGISLATION – AUSTRALIA

The exposure draft for legislation to cover the government's personally controlled e-health record program, issued in September 2011, contains provisions worth consideration by information security professionals. [65]

The draft legislation is to be introduced to support the introduction of an eHealth System in Australia. The system is based on the concept of a "personally controlled electronic health record" (PCEHR) which is an electronic record of a consumer's medical history, stored and shared in a network of connected systems. The PCEHR will bring key health information from a number of different systems together and present it in a single view. The eHealth system to be established will mean that information in a PCEHR can be accessed by the consumer and their authorised healthcare providers, nominated family members and carers whilst enabling the consumer to control who can access their PCEHR. With this information available to them, healthcare providers can make better decisions about a consumer's health and treatment advice. Consumers can contribute to their own PCEHR and add to the recorded information stored in their PCEHR.[66] In short, the Commonwealth eHealth system which is intended to enable the secure sharing of health information between an individual's healthcare providers, whilst enabling the individual to control who can access their PCEHR. The System is being designed to use healthcare identifiers to support the accurate linkage of records to consumers and providers.

This legislation will establish a strict security system to protect the privacy of patients using the eHealth system. Patients will not only be able to access their own eHealth record but will also be able to view who has accessed their record. The legislation requires proactive monitoring of the system to detect suspicious or inappropriate behaviour, ensuring that records are only accessed when there is a need to do so.

The legislation includes strong penalties of up to $66,000 for a record being inappropriately accessed. If more than one record is accessed without authorisation then the penalty multiplies by the number of records.

To participate, consumers will be required register for a personally controlled eHealth record. As well as viewing their own records, patients can add their own notes about their general health but cannot make medical notes. Patients can also upgrade their privacy settings to suit their needs. Doctors, or other health professionals, will be the only people allowed to create medical notes on the file.

The Minister's expectation is that the PCEHR System will be "more secure and private" than paper-based records.[67]

---

[65] Exposure Draft "Personally Controlled Electronic Health Records Bill 2011"

[66] From Minter Ellison, "*Privacy Impact Assessment Report Personally Controlled Electronic Health Record (Department of Health and Ageing)*" November 15, 2011 Chapter 2 at p12 http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-legals-pia/$File/PCEHR-Privacy-Impact-Assessment-Report.pdf

[67] Brett Winterford "**Fines levied for e-health data breaches" September 30, 2011 IT News** http://www.itnews.com.au/News/275292,fines-levied-for-e-health-data-breaches.aspx Last accessed 4 October 2011

Breach Notification

The proposed legislation requires notification where an organisation hosting an information repository or portal operator or a health authority becomes aware of either:

- An unauthorised collection, use or disclosure of health information; or
- An event has occurred or circumstances have arisen (whether or not involving a contravention of the Act) that compromise or may compromise the security or integrity of the PCEHR system[68]

State organisations must notify the relevant State authority. Otherwise, the organisation must notify both the health service provider (where the IT company becomes aware of the breach) and the Information Commissioner. System Operators must notify the Australian Information Commissioner. In both cases the notification must be "as soon as practicable after becoming aware of the contravention, event or circumstances.[69]

There are a series of mandatory actions to be taken as soon as practicable after becoming aware of the incident. These include:

- contain the leak and undertaking a preliminary assessment of the causes
- evaluation of the associated risks
- consider notifying affected consumers
- take steps to prevent or mitigate the effects of the breach re-occurring.[70]

A contravention of this provision is not a civil penalty provision – although it may have other consequences such as the cancellation of registration enabling participation in the system.

There has been considerable response to the proposed draft.

The Privacy Commissioner **reportedly has called for a unified approach to privacy protections in his response to the draft legislation,**[71] **calling for** clear privacy protections. Although the legislation specifies that a contravention of that Act will be taken to be an interference with a person's privacy for the purposes of Schedules 3 and 3A of the Privacy Act,[72] the Commissioner has asked for clarification of how the different commonwealth, state and territory privacy laws will apply. He also called for stronger powers for the Office of the Australian Information Commissioner to audit the system operator, open "own motion" investigations and investigate anyone who may have contravened a civil penalty provision and manage the complaints process.
The Australian Privacy Foundation is a strong critic of the proposal – having issue with, among other things:

- The failure to address new and emerging technologies such as cloud computing and smart phones. The APF maintains that the legislation "must specify guidelines or standards to enable to application of new and emerging technologies to the PCEHR system."[73]
- The absence of penalty provisions where no deliberate data breach has occurred.

---

[68] Section 67(1) Exposure Draft "Personally Controlled Electronic Health Records Bill 2011"
[69] Sections 67(2) and (3) Exposure Draft "Personally Controlled Electronic Health Records Bill 2011"
[70] Section 67(4) Exposure Draft "Personally Controlled Electronic Health Records Bill 2011"
[71] Karen Dearne "E-health record plan must be uniform, says privacy commissioner" November 8, 2011, The Australian http://www.theaustralian.com.au/australian-it/government/e-health-record-plan-must-be-uniform-says-privacy-commissioner/story-fn4htb9o-1226188093410 Last accessed 8 November 2011
[72] See Exposure Draft, Section 64 – 65 Division 3 - Interaction with the Privacy Act 1988 at p44
[73] Australian Privacy Foundation "APF feedback about the exposure draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011" October 27, 2001 at www.privacy.org.au

An independent Privacy Impact Assessment of the proposed system was undertaken by Minter Ellison law firm and released in November 2011.

Unfortunately, the Report did not cover information security aspects of the system – stating that the report did not include "an assessment of the adequacy of information security arrangements for the proposed PCEHR System."74

AUTHOR	
Jodie Siganto, LLM, CISSP. Jodie graduated as a lawyer in 1984 and after 8 years in private practice took the position of in-house counsel for Tandem Computers followed by roles with Unisys Asia and Dell based in Singapore. She returned to Australia in 2000, establishing Bridge Point Communications (specialists in data networking and security) with two other colleagues. She is currently a director of IT Security Training Australia, an (ISC)2 educational affiliate, specializing in the delivery and development of IT security and network related training courses around Australia. In addition, Jodie is currently completing a PhD at QUT in Information Security Law.	
CONTACT DETAILS	E: Jodie_siganto@itsecuritytraining.com.au P: 1300 412 050 M: 0408 275 733 www.itsecuritytraining.com.au

[74] Minter Ellison, "Privacy Impact Assessment Report Personally Controlled Electronic Health Record (Department of Health and Ageing)" November 15, 2011 Chapter 1 Section 1.1.2 at p7 http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-legals-pia/$File/PCEHR-Privacy-Impact-Assessment-Report.pdf