Australian Government

Attorney-General's Department

May 2013

Regulation Impact Statement

Privacy Act 1988

Privacy Alerts

(Mandatory Data Breach Notification)

Background

Australian Law Reform Commission report on privacy

In May 2008, the Australian Law Reform Commission (ARLC) concluded a 28-month inquiry into the effectiveness of the *Privacy Act 1988* (Privacy Act) and related laws as a framework for the protection of privacy in Australia[1]. In its report, the ALRC made 295 recommendations for reform in a range of areas, including creating unified privacy principles, updating the credit reporting system, and strengthening the powers of the Privacy Commissioner. The Government has responded to the majority of their recommendations through the passage of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* in Parliament in December. As a result of that Act, major privacy reforms will commence in March 2014.

One of the ALRC's other recommendations was that a mandatory data breach notification scheme be introduced (rec 51-1). The ALRC noted that, with advances in technology, entities were increasingly holding larger amounts of identifying information in electronic form, raising the risk that a breach of this information could result in another individual using the information for identity theft and identity fraud. Stalking, embarrassment, or discrimination can also sometimes result from the unauthorised release or loss of information held by an agency or organisation.

Submissions to the ALRC's inquiry indicated strong support for the introduction of a mandatory requirement, although some key private sector organisations were not supportive such as banks and telecommunications providers[2].

Under the Office of the Australian Information Commissioner's (OAIC) guide '*Data Breach Notification: A guide to handling personal information security breaches*', a data breach is defined as the situation where 'personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure, or

[1] See at: http://www.alrc.gov.au/publications/report-108
[2] See ALRC Report (paras 51.52 – 51.56)

other misuse'[3]. The OAIC guide notes that breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow information-handling policies that cause accidental loss or disclosure. The OAIC guide provides some common examples:

- lost or stolen laptops, removable storage devices, or paper records containing personal information;
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased;
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organisation;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins;
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

The ALRC believed that the key objective of a notification requirement is that it would allow individuals whose personal information had been compromised by the breach to take remedial steps to lessen the adverse impact that might arise from the breach. The ALRC believed that, by arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitor their accounts, or take preventative measures such as change passwords and cancel credit cards.

A mandatory scheme would also encourage agencies and organisations to be transparent about their information-handling practices, and result in an improvement in compliance with privacy obligations. The reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives to improve security. On the other hand, reputational damage is often cited as

[3] See at: http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html#_Toc301281660

a reason why some private sector organisations do not notify regulators or affected individuals about data breaches.

The ALRC noted that the Privacy Act contained requirements for the handling of personal information that are relevant to the issue of data breach. It noted that a data breach may occur because an agency or organisation has failed to comply with its obligations in regards to the use and disclosure of personal information, or where it had failed to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. However, a data breach may also occur where an agency or organisation has been in compliance with the Privacy Act but the information it holds has been stolen or 'hacked' into.

A recent example of this can be found in the Privacy Commissioner's report on an investigation into a major data breach on the Sony PlayStation Network / Qriocity[4]. In that case, the Privacy Commissioner was satisfied that, at the time of the incident, 'reasonable steps' had been taken by the company involved in accordance with the requirements of the Privacy Act. Those reasonable steps ensured that customers' personal information was secure and protected from misuse and loss, and from unauthorised access, modification and disclosure. However, the Privacy Commissioner also commented that affected individuals could have been notified earlier, rather than seven days being allowed to elapse after the discovery of the cyber-attack. The Privacy Commissioner believed that the delay may have increased the risk of a misuse of the personal information of affected individuals.

The ALRC also noted developments in international jurisdictions where legislative reform has been implemented. For example, nearly all US states have implemented some form of mandatory data breach notification legislation, and steps have been taken to consider a national model. Since the ALRC report and the release of the Government's discussion paper (noted below), the European Union has also announced proposals to require companies to disclose certain data breaches within 24 hours of their occurrence. Therefore, the trend in international jurisdictions appears to be moving

[4] See at: http://www.oaic.gov.au/publications/reports/own_motion_sony_sep_2011.html

towards the development and implementation of legislative requirements for notification of data breaches.

After considering submissions and consultations, the ALRC recommended that a data breach notification requirement be introduced in the Privacy Act. The ALRC considered that the test should set a higher threshold for notification than is provided in most other tests (ie a test based on a real risk of serious harm to an affected individual). Amongst other things, the ALRC believed that a higher threshold for notification should also reduce the compliance burden on agencies and organisations.

The ALRC believed that the agency or organisation should decide on whether the triggering event has occurred. This will allow organisations and agencies to develop their own standards about what constitutes a real risk of serious harm in the context of their own operations.

The ALRC also believed that it would be appropriate to allow for a civil penalty to be imposed where an agency or organisation has failed to notify the Privacy Commissioner of a data breach. The rationale behind this recommendation was that it would provide a strong incentive for agencies and organisations to disclose data breaches where required, and encourage these entities to consult with the OAIC where a data breach has occurred to ensure they are in full compliance with the requirements.

The ALRC's recommendation (51-1) in full is at **Attachment A**.

Government response

On 14 October 2009, the Government released a First Stage Response to the Australian Law Reform Commission's report, which committed to address 197 of the Commission's 295 recommendations. Recommendation 51-1 was not part of the 197 recommendations and was identified along with a number other recommendations as requiring more consultation and consideration.

Discussion paper

On 19 October 2012, the Government released a discussion paper seeking public comments on whether Australia's privacy laws should include a mandatory data breach notification requirement and, if so, the possible elements of such a requirement. The

content of the discussion paper and the responses to it are outlined and analysed in more detail in the 'Impact Analysis' and 'Consultation' sections below.

Further targeted consultation

In April 2013, the Government undertook confidential targeted consultation on a more detailed legislative model. This consultation process invited comments on the legislative model, and sought particular views on the possible costs on business. Further details of this consultation are outlined and analysed in more detail in the 'Impact Analysis' and 'Consultation' sections below.

Assessing the problem

Magnitude

The ALRC found that, with advances in technology, agencies and organisations are storing vast amounts of identifying information electronically. The increased use of the internet and other current and emerging mobile technologies pose new challenges for privacy protection, as Australians increasingly transact commercially and engage socially in the online environment. Personal information such as medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work are increasingly transitioning to web pages and data centres, with varying degrees of accessibility and security.

There are studies and anecdotal evidence suggesting that breaches of data security are increasing in frequency and scope.[5] Some recent US reports have found that up to 88 per cent of organisations surveyed have had at least one data breach during the course of a year[6]. In its most recent annual report about incidences of data breaches, Verizon found that there had been a large spike in the number of incidents, and that 98% of these incidents were caused by outside parties, such as hackers[7]. A more recent Australian survey found that more than 20% of surveyed businesses to admitted to data breaches[8].

[5] www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf
[6] http://www.symantec.com/about/news/release/article.jsp?prid=20101117_01
[7] http://www.verizonenterprise.com/resources/reports/es_data-breach-investigations-report-2012_en_xg.pdf
[8] http://www.zdnet.com/au/australian-organisations-unprepared-for-new-privacy-laws-mcafee-7000014636/

In a recent media article from Canada, it was reported that the Canadian Federal Government had experienced more than 3,000 data and privacy breaches over the past 10 years, breaches that have affected more than 725,350 Canadians[9]. The same article reported that this was not a complete accounting of breaches, suggesting that there the number of breaches may be higher than reported. The list also turned up at least three instances where the data loss led to criminal activity.

The harm impact on consumers from data breaches could include financial loss, and psychological and physical harm.

An example of financial loss occurred in the February 2005 case involving the data broker, ChoicePoint, which disclosed a security breach, as required by the California Security Breach Act, involving the personal information of 163,000 persons[10]. According to the US Federal Trade Commission, ChoicePoint employees were duped into handing over sensitive data of consumers to an organised identity theft ring, which resulted in at least 800 victims having their names, addresses and social security numbers used for a variety of unauthorised purposes. A settlement order was entered into in 2006 by ChoicePoint with the FTC including a commitment to improve privacy procedures. In October 2009, ChoicePoint settled charges that it violated the 2006 settlement order and agreed to a modified court order that expanded its data security assessment and reporting duties, and required the company to compensate affected consumers for the time they may have spent monitoring their credit or taking other steps in response[11].

In Australia, there are fewer examples that estimate, or show, the links between data breaches and activities that can cause serious harm to individuals such as identity theft. The Centre for Internet Safety at the University of Canberra has estimated that the potential for personal or business data to be stolen had grown in recent years, with a decline in the prices charged by cyber criminals for access to data such as credit card details[12].

---

[9] http://www.canada.com/Government+data+breached+thousands+times+last+decade+documents/8284404/story.html
[10] See at: http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf
[11] http://www.ftc.gov/opa/2010/09/choicepoint.shtm
[12] http://www.cio.com.au/article/418590/call_mandatory_data_breach_notifications_renewed/

In terms of whether a notification scheme would operate to limit the harmful effects of a data breach, some private sector stakeholders in responses to the Discussion Paper and in the targeted consultation process queried whether there was empirical evidence to suggest that notification of itself has been effective in reducing the likelihood or impact of a data breach in overseas countries. This observation was reiterated by some industry groups in responding to the targeted consultation process.

The US cases are limited but provide some evidence on this issue. Of the limited studies to date, there is empirical evidence to show that notifying affected consumers can reduce harmful effects such as identity theft. A 2008 study appeared to show that connection between data breaches and identity theft does exist. In that paper, a study of US jurisdictions using data from between 2002 and 2007 showed that the adoption of data breach notification laws 'reduce the identity theft rate by just 2%, in average'. Although this figure may seem low, a 1.8% reduction in identity theft would lead to savings of approximately $US1 billion. When that study was updated in 2011, the conclusion was that, based on data from 2002 to 2009, an empirical analysis revealed that these laws have reduced identity thefts by about 6.1%[13]. It is therefore open for the conclusion to be drawn that data breach laws are a longer term effective measure in combating identity theft.

In terms of the size of harm that consumers may experience, there is no information to accurately quantify that impact on consumers in Australia.

While annual studies undertaken by Verizon and Symatec appear to indicate that that there is an increase in the number of data breaches, the actual amount of under-reporting of these breaches is difficult to quantify. However, there is some anecdotal evidence that this is occurring. For example, the Privacy Commissioner has publicly stated that, based on media reports citing information technology security experts, the OAIC has only been notified of a small percentage of data breaches that are occurring[14]. In its submission to the Discussion Paper, the Centre for Internet Safety also asserted that significant amounts of underreporting had been occurring.

---

[13] See at: http://www.truststc.org/pubs/831/SSRN-id1268926.pdf

[14] http://www.oaic.gov.au/news/media_releases/media_release_121017_mdbn_paper.html

In its submission to the Discussion Paper, the Victorian Privacy Commissioner noted that data breach notifications to the OAIC increased 27 per cent in the previous financial year (i.e. from 2009/2010 to 2010/2011). However, in the most recent reporting period (2011/2012) data breach notifications decreased 18 per cent. Respondents to the discussion paper have argued that this may lead to the conclusion that underreporting is occurring because the number of reports should be increasing in proportion with the increasing number of larger scale data breaches.

On the other hand, some respondents to the discussion paper have argued that the lack of clear information about the level of underreporting shows that there is no evidence of regulatory or market failure that has created a consumer protection risk warranting a response. Further, the response to the discussion paper revealed that attempting to quantify the problem is difficult because many organisations do not have the capability of detecting whether data loss has occurred, and whether there has been a significant impact or harm caused by such data loss.

Data breach notification schemes are generally underpinned by the notion that only those breaches that give rise to the likelihood of serious harm should be reported. One problem is that individuals have different attitudes to privacy protection and some are less concerned about the risks of providing large amounts of personal information, and may react differently to the idea that their personal information may be compromised[15]. This is particularly the case if the information that is accessed or disclosed is likely to cause some form of psychological harm. Therefore, the views about what is 'serious harm' to someone can be varied, and difficult to quantify.

Existing regulation

There is no requirement under the Privacy Act to notify the OAIC or any other individual in the event of a data breach. If an entity does not contact the OAIC and implement the guidelines, it does not face a legal sanction.

Under the Privacy Act, agencies and organisations are subject to requirements to provide adequate security protection to personal information in their possession. These are

[15] See recent study commissioned for European Commission at: http://ict-endorse.eu/?p=539

contained in the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs), which both require entities to take reasonable steps to protection personal information from misuse, loss or unauthorised access, modification, or disclosure[16].

Section 18G(b) of the Privacy Act imposes equivalent obligations on credit reporting agencies and all credit providers. Similarly, guideline 6.1 of the statutory Tax File Number (TFN) guidelines requires TFN recipients to protect TFN information by such security safeguards as are reasonable in the circumstances[17].

In March 2014, new reforms will come into effect including the commencement of the Australian Privacy Principles (APPs), which will create one set of privacy principles for agencies and organisations. New APP 11, will replace NPP 4 and IPP 4, and require agencies and organisations (known as APP entities) to take such steps as are reasonable in the circumstances to protect the information from:

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

The OAIC's view is that notification may be a 'reasonable step' where a data breach has occurred. However, it believes an express mandatory data breach notification law would provide agencies and organisations with greater clarity and certainty regarding their obligation to notify, and the circumstances in which notification should be made.

These data security requirements are aimed at encouraging entities to provide sufficiently high levels of security to minimise the possibility that personal information could be compromised. Provided an entity implemented these requirements, it would not be in breach of its existing Privacy Act obligations, even if it suffered a data breach involving large amounts of personal information.

In the absence of a legal requirement, entities are encouraged to adhere to the OAIC data breach notification guide. The guide provides general guidance on key steps and factors for agencies and organisations to consider when responding to a data breach involving

---

[16] *Privacy Act 1988* - NPP 4 and IPP 4

[17] See at: www.oaic.gov.au/publications/guidelines/Guidelines-TFN.pdf

the personal information that they hold. That guide provides some guidance around the Privacy Act obligation to put in place reasonable security safeguards and to take reasonable steps to protect the personal information from loss and from unauthorised access, use, modification or disclosure, or other misuse. Depending on the circumstances, those reasonable steps may include the preparation and implementation of a data breach policy and response plan.

The OAIC guide contains 4 key steps for an agency or organisation to take when a data breach occurs. These are: (1) Contain the breach and do a preliminary assessment; (2) Evaluate the risks associated with the breach; (3) Notification; and (4) Prevent future breaches.

A key issue is whether the voluntary OAIC guide is operating as an effective means to encourage widespread notification of breaches. As noted above, there has been an 18% decrease in 2011-12 from the number of data breach notifications received in 2010–11[18]. The Privacy Commissioner has commented that that this decrease in notifications was difficult to explain but noted that media reports citing information technology security experts had suggested that only a small percentage of data breaches were being notified to the OAIC.

Although there are arguments noted above that claim this is evidence that data breaches are decreasing in frequency, there are figures in other studies indicating that there has been an increase in breach incidents (see Verizon and Symantec reports referred to above). These studies indicate that there are more entities holding larger amounts of personal information in electronic form, and the incidence of hacking (which are the cause of most data breaches) are generally agreed to be on the increase.

There are some high-profile cases to date where the issue of providing timely notification has been considered important. For example, as noted above in the Sony PlayStation Network / Qriocity[19] investigation, the Privacy Commissioner commented that affected individuals could have been notified earlier, rather than seven days being allowed to elapse after discovering the cyber-attack had occurred. The Privacy Commissioner

[18] http://www.oaic.gov.au/news/media_releases/media_release_121017_mdbn_paper.html
[19] See at: http://www.oaic.gov.au/publications/reports/own_motion_sony_sep_2011.html

believed that the delay may have increased the risk of a misuse of the personal information of affected individuals.

Relevant risks

A key risk is that an ineffective regulatory framework may raise challenges in encouraging community confidence to fully participate in the continued growth of e-commerce and the digital economy. Studies show that individuals have significant privacy concerns related to the handling of personal information, particularly in the online environment[20]. A key element in the Government's digital economy strategy is to provide for a safe and secure online environment for Australian users[21]. That will assist Australian businesses to harness and fully realise the potential that developments in information and communications technologies enable.

For example, respondents to a survey published by the Centre for Internet Safety at the University of Canberra indicated that perception on privacy is a determinant in their online activities, particularly their decision to buy and sell goods and services online[22]. Respondents rated identity theft (86%) and loss of financial data (83%) as their areas of greatest privacy concern online. The study also found that 85% of Australians believed that data breach notification should be mandatory for business.

In its submission to the Discussion Paper, the Australian Information Security Association (AISA) advised that 78% of members who commented on the issues in the paper reported that general information and communications technology staff do not have the necessary skills to securely design or operate information systems that store or process information assets. The AISA further advised that 62% of their respondent members thought that their organisations did not fully appreciate the security threats they faced. This suggests that increased transparency about data breach incidents may assist in the development of appropriate measures to combat them in the future, and improve awareness amongst entities about the threats.

---

[20] See recent study commissioned for European Commission at: http://ict-endorse.eu/?p=539

[21] http://www.cybersmart.gov.au/About%20Cybersmart.aspx

[22] http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf

There is also a risk that Australian businesses could leave themselves in a position to suffer financial loss. For example, in its submission to the Discussion Paper, the Australian Institute of Criminology noted that while there are benefits to an individual in early detection of data breaches, 'these benefits may also carry over to financial institutions and other businesses with early fraud detection reducing financial loss and saving time in the long term'.

Potential for market development

In response to the discussion paper, a number of private sector stakeholders argued that private sector organisations have developed good privacy practices since the application of the Privacy Act to the private sector in 2001, and understand the importance of seeking the assistance of the OAIC where appropriate and in dealing with the privacy concerns of their customers. They also argue that, contrary to anecdotal reports, there is no real evidence in Australia of underreporting of significant data breaches to the OAIC, or not at the level to warrant a legislative requirement.

Respondents to the discussion paper believe there are existing commercial incentives for providing high level security and for prompt responsiveness in the event of a significant data breach. Consumers have identified security as a major privacy issue and may be less likely to transact with a company that has lax privacy protection record, or has inadequate privacy policies[23]. If consumer perceptions and behaviours develop in this way, that may drive private sector companies to develop better privacy practices (ie a 'market solution'), including notification of data breaches.

Objectives of government action

The existing Privacy Act does not include an objects clause, although section 29 of the Act requires the Privacy Commissioner to have regard to a number of matters in performing his or her functions. These include the protection of important human rights and social interests that compete with privacy such as the general desirability of a free flow of information, through the media and otherwise, and the right of government and business to achieve their objectives in an efficient way.

[23] http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf

From March 2014, the Privacy Act will contain new objectives. These will be to promote the protection of privacy of individuals, while recognising that this protection should be balanced with the interests of entities carrying out their legitimate functions or activities.

In its submission to the Discussion Paper, the Australian Finance Conference (AFC) noted that there are complementary objectives at play in establishing a balanced privacy regulatory framework, including a data breach requirement that impacts on business. It noted that an appropriate combination of the Government's consumer protection and digital economy objectives will enable a robust and adaptable privacy framework, in an environment where AFC members and others are able to boost their productivity and global competitiveness by realising the potentials offered by technological advances.

A key outcome of a well-balanced privacy framework is the provision of a safer and more transparent environment for Australians to entrust their personal information to agencies and organisations. Greater assurance about the safety of personal information will encourage consumers to more fully engage in e-commerce, thereby boosting Australia's digital economy.

Another goal of privacy policy is to enable an enhanced information and assessment process to better inform policy makers, regulators, law enforcement and researchers about trends in the handling of personal information.

Option one – Retain the status quo

Option 1 is to maintain the status quo. This means that entities subject to the Privacy Act will have no legal obligation to report a breach of personal information. They will continue to be encouraged to comply with the existing OAIC guide on data breach notification.

The OAIC guide provides general guidance on key steps and factors for agencies and organisations to consider when responding to a data breach involving the personal information that they hold. That guide notes that, agencies and organisations have obligations under the Privacy Act to put in place reasonable security safeguards and to take reasonable steps to protect the personal information that they hold from loss and

from unauthorised access, use, modification or disclosure, or other misuse. Depending on the circumstances, those reasonable steps may include the preparation and implementation of a data breach policy and response plan (that includes consideration of whether to notify affected individuals and the OAIC).

In response to the discussion paper, a number of private sector stakeholders argued that the voluntary scheme was sufficient in encouraging the reporting of significant breaches and in giving guidance to entities about how to effectively respond to these breaches. Many argue that private sector organisations have developed good privacy practices since the application of the Privacy Act to the private sector in 2001, and understand the importance of seeking the assistance of the Privacy Commissioner where appropriate and in dealing with the privacy concerns of their customers. They also argue that, contrary to anecdotal reports, there is no real evidence in Australia of underreporting of significant data breaches to the OAIC. Additionally, some argue that mandatory data breach notification laws effectively penalise regulated entities, which are often the targets of cybercrime attacks.

Maintaining the status quo would also allow the market participants to continue to develop good privacy practices consistent with the expectations of their customers. It is arguable that there is a sufficient commercial incentive for organisations to implement good privacy practice and notify their customers in the event that their information may become compromised. The reputational costs that come with failing to respond properly to significant data breaches are a strong incentive to notify the OAIC and consumers about breaches. In the current digital economy, consumers are more likely to consider the privacy track record and policies of a business when deciding whether to entrust it with their personal information[24].

There are also new privacy reforms that will commence in March 2014. These will give the Privacy Commissioner the power to audit private sector organisations and potentially discover data breaches. That will potentially make it more difficult for an entity to hide the data breach. For reputational risk reasons, that is also likely to provide an incentive to report data breaches to the Commissioner and affected individuals.

[24] http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf

Option two – Introduce a mandatory data breach notification scheme

Option 2 is to introduce a legal requirement for entities to report data breaches to the OAIC and to affected individuals where the breach gives rise to a real risk of serious harm to an affected individual. There would be a number of objectives underpinning such an approach.

The proposed model would apply the data breach notification law to all entities currently regulated by the Privacy Act. There was general support for this approach from respondents to the discussion paper. This would not include entities, or some of their activities, that fall within exemptions in the Privacy Act, such as most small businesses, political parties and media organisations.

The proposed model would implement the ALRC's recommended trigger for notification, which was a test based on a 'real risk of serious harm' to an affected individual. This would not be a remote risk and would therefore not require entities to report less serious privacy breaches to affected individuals or the OAIC. This was consistent with the views of the clear majority of submitters who commented on this issue.

The requirement to notify would apply to personal information held by APP entities, credit reporting information held by a credit reporting body, credit eligibility information held by credit providers, and tax file number information held by file number recipients. Where these types of information have been disclosed to foreign recipients, the requirement to notify will remain with the disclosing Australian entity in certain circumstances.

In the targeted consultation process, there was support expressed for more explanation about, or a definition of what constituted 'serious harm'. Without this additional assistance, it was argued that some regulated entities may adopt a more risk adverse approach to notification by taking a narrow interpretation. The consequence may be that the standard of notification would not be high enough to avoid notification fatigue and

create resourcing issues at the OAIC. As a consequence of these comments, further material will be included in the Explanatory Memorandum to the Bill.

The ALRC recommended that the entity involved in the breach should have the responsibility of notification. Most respondents to the Discussion Paper generally favoured this approach noting that the entity was best placed to assess the breach, the adverse risks that might arise, and what mitigating action could be taken. The proposed model incorporates this approach.

The proposed model would also give the OAIC the power to compel notification to affected individuals. This measure will enable affected individuals to be notified if an APP entity does not notify but where the OAIC considers that there is a 'real risk of serious harm to any affected individual'.

On the content of the notification, there were a range of views with private sector submitters preferring less detailed information having to be provided, while privacy commissioners and privacy advocates believed more information should be included.

The ALRC recommended that, as a minimum, the notification should contain: a description of the breach; a list of the types of personal information that were disclosed; and contact information for affected individuals to obtain more information and assistance. The approach in the proposed model incorporates these suggestions and also requires information about the practical implications of the breach to be included. These are based on the existing OAIC voluntary standards. Given that there are matters of detail that could evolve over time, the proposed model includes the power to prescribe additional notification matters in regulations.

There was general support from stakeholders that the means of notification should be directly by phone, letter, e-mail, in person, or by normal means of communication between the entity and the individual. If direct communication is not practicable, a requirement to publish in a newspaper (similar to a recall notice) will be applicable. In the target consultation process, industry groups expressed the wish for flexibility so that regulated entities could notify individuals in a variety of ways. This would enable a more timely notification to an individual (eg by phone) than their usual form of communication with that entity (eg by mail). It would also be a measure that could

reduce the costs burden on entities. This suggestion has been incorporated into the proposed Bill.

The proposal legislation also provides that entity should be required to notify as soon as practicable after it believes on reasonable grounds that there has been a breach. Most discussion paper submitters believed that flexibility, rather than a set time frame, was needed given the variable factors unique to each data breach.

The proposed legislation enables the Privacy Commissioner to exempt an entity from the requirement to notify a data breach where the Commissioner is satisfied that it is in the public interest to do so.

The proposed legislation would link into the elevated penalty structure in the existing Privacy Act where less severe sanctions could be used before elevating to a civil penalty. These less severe penalties could follow a Privacy Commissioner investigation and include public or personal apologies, compensation payments or enforceable undertakings. A civil penalty would only be applicable where there has been a serious or repeated non-compliance with mandatory notification requirements.

Option three – Encourage industry to develop industry codes

Option 3 is to encourage entities regulated under the Privacy Act to develop industry codes that provide a self-regulatory framework tailored to particular industry needs, taking into account existing reporting requirements and compliance issues. This could be complemented with increased efforts on the part of the OAIC to promote more awareness about the OAIC guide.

Some industry groups have developed self-regulatory codes as a tool to promote standard practices and compliance. For example, the Association for data-driven marketing and advertising (ADMA) has developed a Code of Practice to set standards of conduct for direct marketers, minimise the risk of breaching legislation (including the NPPs in the Privacy Act), promote a culture of best practice, serve as a benchmark in settling disputes and increase business and consumer confidence in doing business with ADMA members who are bound to the provisions of the Code.

Studies from the US indicate that the per capita cost of data breach incidents is different for particular industries with the telecommunications, pharmaceutical, financial and healthcare industries incurring higher costs. This may support the argument that particular industries are in a better position to identify what is reasonable in terms of developing their own data breach responses having regard to their own compliance cost issues.

On the other hand, there were mixed views provided by key Australian industry groups in the targeted consultation process. Some believed that there would be no disproportionate adverse impact on different industry groups, while others believed that small businesses (ie those subject to the Privacy Act because they trade in personal information) would be affected in that way.

While the Privacy Act allows the development of codes which, in theory, would allow particular industries to develop a more tailored approach to personal information-handling, these are not intended to derogate from minimum standards set out on the IPPs and NPPs (and APPs). Under the new reforms, they will be required to be registered by the OAIC and this is unlikely to occur if the code purports to implement inadequate standards (eg if they contained standards less than the OAIC guide).

This option could be complemented with increased efforts on the part of the OAIC to promote more awareness about the OAIC guide, and the importance of complying with it as good privacy practice. For example, the OAIC has recently finalised an updated *Guide to Information Security*, which was released by the Attorney-General at the beginning of Privacy Awareness Week 2013 in April 2013[25]. In any self-regulatory framework, the regulator's suggested standardised rules would be a useful starting point.

[25] http://www.oaic.gov.au/publications/guidelines.html#other_privacy_guidance

Impact analysis

Option 1

Agencies and private sector organisations under the Privacy Act will continue to operate in accordance with the IPPs and NPPs (and new APPs from March 2014), and be encouraged to continue to report significant data breaches to the OAIC and affected individuals. Some of these bodies will become subject to more enhanced privacy requirements in March 2014, including new auditing powers for the OAIC in relation to private sector organisations. These measures are expected to increase transparency thereby making it more difficult for entities to prevent discovery of significant data breaches. Public perceptions about responses to data breaches are likely to remain in favour of prompt reporting, which may drive the development of stronger security measures and increased compliance with the voluntary OAIC guide.

Impact on OAIC

Under this option, there is likely to be little impact on the OAIC itself, except that it will have enhanced powers to discover breaches from March 2014. More information about breaches is also coming to light with hackers now publicly reporting on their efforts. The OAIC will be able to seek stronger sanctions in responding to them (eg enforceable undertakings and civil penalties), which could act as a deterrent against lax security standards. The OAIC guide may require minor amendments but mainly to reflect the OAIC's new powers in relation to breaches of the Privacy Act. Should legislation not proceed, there may be re-doubled efforts to publicise and encourage compliance with the OAIC guide, which will impact on the public education/awareness resources of the OAIC.

Impact on individuals

There will be little change for individual Australians noting that they face existing risks without a mandatory scheme. There remains a possibility that they may continue to not be informed in the event that their personal information becomes compromised, thereby raising the risk they could suffer serious harm. Their expectations may be raised that, with the commencement of an enhanced privacy protection regime, and with more focus

on information security issues, entities will increasingly comply with the OAIC guide. As noted above, more undisclosed breaches may begin to come to light because of the Commissioner's new powers, and the trend in hackers revealing their work. Studies show that the public are in favour of being notified in the event of a data breach affecting their personal information, and this may encourage more entities to err on the side of reporting where there has been a breach.

There will be no impact on small businesses as they are generally not subject to the Privacy Act. Larger not-for-profit organisations who are subject to the Privacy Act (because they have a turnover of greater than $3 million) will be in the same position as organisations who are subject.

Option 2

Agencies and private sector organisations under the Privacy Act will be required to update their internal privacy practices to incorporate a requirement to notify the OAIC and affected individuals in the event of a data breach. While many entities have updated internal systems to factor in a notification cost component to enable compliance with the OAIC guide, not all would have done so given that it is a voluntary scheme only. In response to the targeted consultation process, industry group respondents commented that it would be hard to judge whether there would be any incremental increase in cost to entities that already have systems in place to comply with the OAIC guide.

Impact on individuals

Dealing with adverse effects – identity theft

Mandatory data breach notification laws are intended to provide notification to a person who has had their privacy infringed by the breach about the incident, and information about steps that can be taken to mitigate the harm that might be caused by the breach. That person will have an opportunity to take corrective action to change or otherwise 'resecure' the information. The ALRC considered that this could be referred to as the 'mitigation objective'.[26] For example, this might allow an individual to change

[26] See further ALRC report (2008), para 51.77-51.78.

passwords where those passwords have been hacked, to cancel credit cards if details have been stolen, or to change telephone numbers where silent numbers have been revealed.

However, such a rationale shifts the onus away from the organisation that has suffered the breach and onto a person who may be ill-equipped or unable to correct the consequences of the breach. For example, in cases where an individual's health information has been accidentally uploaded to the internet, it may not be possible to rectify the breach even if it has been subsequently taken down. Once that information has been disclosed, knowledge about it may become widespread.

Provided there is improved compliance as expected, individual Australians will be informed in the event that their personal information becomes compromised, allowing them to take appropriate action to mitigate harm. That is expected to raise confidence amongst consumers about the entities that they are dealing with, and the increased transparency will provide them with more information to make informed choices about which entities they want to transact with. There is the possibility that some entities that need to make internal changes to meet compliance could pass those costs on to consumers thereby making transactions more costly.

In terms of the impact on the Australian community as a whole, there may be benefits in developing measures to combat cybercrime and through greater transparency in personal information handling. Notifications can also enable law enforcement, researchers, and policy makers to better understand which firms and business sectors are better (or worse) at protecting consumer and employee data[27].

Impact on businesses

Requiring notification may act as an incentive to the holders of personal information to adequately secure or dispose of that information. In other words, the adverse publicity occasioned by a notification may deter poor handling of such information, and increase the likelihood that adequate and reasonable measures are taken to secure it. This could thus be called the 'deterrent objective'. The ALRC viewed this as more of a secondary

[27] See; http://www.truststc.org/pubs/831/SSRN-id1268926.pdf at page 5.

objective, although it has been part of the rationale for data breach notification laws in many other jurisdictions.

A mandatory notification scheme may result in improved compliance with rules relating to the collection and retention of personal information. First, an entity is likely to more carefully consider what personal information is it necessary to collect. As noted in the OAIC guide, personal information that is never collected, cannot be mishandled. The new APPs will require that private organisations only collect personal information that is reasonably necessary for one or more of their functions or activities.

A mandatory notification scheme will also make entities focus on how long personal information needs to be retained. New APP 11 requires organisations to securely destroy or permanently de-identify information that is no longer needed for the permitted purposes for which it may be used or disclosed. The destruction or de-identification of information that this no longer required will usually be a reasonable step to prevent the loss or misuse of that information.

The creation of mandatory laws would also create a more level playing field for organisations. The Victorian Privacy Commissioner noted that only those ethical and compliance conscious organisations are likely to voluntarily report. Mandatory notification would assist in reducing (and possibly eliminating) incentives for organisations to suppress or deliberately conceal data breaches.

There will be no impact on small businesses which are not subject to the Privacy Act. Under the Privacy Act, a business with an annual turnover of less than $3m is considered a small business, and is generally not required to comply with the Act. However, there are a number of small businesses in that category which are subject to the Privacy Act because of exceptions to the Act contained in provisions such as paragraphs 6D(4)(c) – (d), eg they trade in personal information. In the targeted consultation process, it was argued that there would be a disproportionate cost on these entities, particularly in the direct marketing industry, as they may not be in a position (unlike larger organisations) to absorb some of the costs internally.

Larger not-for-profit organisations who are subject to the Privacy Act (because they have a turnover of greater than $3 million) will be in the same position as organisations who

are subject. A possible negative impact for small business is that individuals may be more tempted to use larger private sector organisations safer in the knowledge that they are subject to mandatory requirements in the event of a data breach.

Specific costs on business

The introduction of a mandatory scheme for entities regulated by the Privacy Act raises the question of what new compliance costs will be necessary. There are no figures outlining the actual numbers of private sector organisations that are subject to the Privacy Act. Around 94% of all private sector organisations are small business operators and therefore generally exempt from the Privacy Act. Certain obligations will apply to small businesses that, for example, trade in personal information, are health service providers, are tax file number recipients, operate residential tenancy databases, or simply voluntarily opt in.

Administrative costs

In the targeted consultation process, respondents from a number of industry groups commented that there would be 'paper burden' or administrative costs in complying with the mandatory scheme outlined above under Option 2. In summary, these were described as:

- costs linked to notification methods (eg mail, telephone, resourcing) so that the actual costs would be incurred by specific business units within an organisation. It was noted that greater flexibility in the notification requirements would assist in containing costs associated with communicating to customers;
- other costs could be in the time and effort in formalising the process (eg internal communications, directives, and process mapping);
- increased insurance costs, which would be a consequence of an increased perceived business risk; and
- costs associated with the need to engage additional legal counsel.

The targeted consultation process did not receive specific costs estimates. There was no common view among respondents about the likely amount of costs, with respondents providing a broad range of general cost estimates on this issue.

For example, one industry group respondent commented that 'larger organisations have stated clearly that the requirements of mandatory notification would involve capital expenditure running into millions of dollars, and the costs would vary depending on the amount of data held by the entity. Another industry group respondent believed there would be 'significant capital costs'.

On the other hand, privacy and consumer advocates argued that the costs would be minimal. These respondents argued that the costs of preventing breaches are in any case generally lower than the costs of handling them once they have occurred; and that it is widely recognised that it is good business practice to proactively manage risks rather than to merely react when something goes wrong. Further, these groups argued that the costs are likely to be mostly one-off and should be considered a normal business overhead for any organisation handling personal information.

For entities that already comply with the OAIC guide, industry group respondents to the targeted consultation process noted that it would be hard to say whether there would be any incremental increase in cost. Privacy and consumer advocate groups argued that costs for these entities are not likely to be significant because they already have systems in place to comply with the existing OAIC guide, and regard responding to security breaches, including through notifying customers, as a necessary part of business.

Effect on particular industry groups

Respondents to the targeted consultation process had mixed views about whether particular industry sectors would incur costs disproportionately through a mandatory data breach notification scheme. Most believed there would be no industry sector impacted disproportionately, although others believed that there would be in the case of:

- small businesses (eg traders in personal information who are subject to the Privacy Act) and start-ups; and
- some members of the financial services sector, given that the coverage includes APP regulated entities, credit providers and tax file number recipients.

Costs of a data breach – US studies

A recent US Ponemon report indicated that the cost of a data breach, both in terms of the organisational cost of data breach and the cost per lost or stolen record have declined,

although the notification component of the cost has increased[28]. The methodology used in this report calculated costs using both the direct and indirect expenses paid by the organisation. Direct expenses included engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates. Using this methodology, an average per capita cost of a data breach in 2011 was $194, which was a drop from $214 in 2010.

The costs associated with notification increased from $0.51 in 2010 to $0.56 in 2011, although still less than $0.66 in 2006 when a large number of data breach laws were introduced in some US states. According to the Ponemon study, these costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up.

There is also a question of the capacity of businesses to implement the reforms at this time. As noted above, AISA advised that 78% of members who commented on the issues in the paper reported that general information and communications technology staff do not have the necessary skills to securely design or operate information systems that store or process information assets. The AISA further advised that 62% of their respondent members thought that their organisations did not fully appreciate the security threats they faced. Instead of regulatory reform there may be value in having a period where education, training and awareness-raising is promoted, so that organisations are better equipped to deal with data breaches, and therefore more likely to comply with a future mandatory scheme.

Mandatory notification laws exist in nearly every state in the United States, and almost 30 of these are based on an original Californian model. That model requires a state agency, or a person or business that conducts business in California, that owns or licenses computerised data that includes personal information, as defined, to disclose in specified ways, any breach of the security of data, as defined, to any resident of

[28] See report available at: http://www.symantec.com/about/news/release/article.jsp?prid=20120320_02

California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. The model used in other US states is based on a trigger for notification only if it is reasonable to believe the information will cause harm to consumers.

This Californian model has a lower threshold than the proposed model in the draft legislation. The proposed amendments would require more serious data breaches to be reported where there is a real risk of serious harm, rather than any breach involving unencrypted personal information. The different approach in the proposed amendments is justified on the basis that the notification burden on agencies and organisations should only be necessary having regard to the interests of the individuals concerned, and it is based on the key threshold already commonly understood by many of these entities in the OAIC guide.

It is therefore possible to conclude that specific costs for entities under the new Australian scheme will be less than under the more stringent Californian model, mainly because reporting is required more often under that model. As noted above, while these costs will be additional for those entities that have not established systems to meet the existing voluntary scheme, for the most part they are not expected to be significant for other entities.

There is some evidence of positive impacts on entities subject to data breach notification schemes in terms of minimising legal liability and negative publicity. In the US, the United States Government Accountability Office**,** reported that representatives of federal banking regulators, other government agencies, industry associations, and other affected parties stated that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimise legal liability or avoid public relations risks that may result from a publicised breach of customer data[29].

Impact on competition

In some discussions with stakeholders it has been suggested that, in the US, bigger companies support data breach laws because smaller competitors cannot meet the

[29] http://www.gao.gov/assets/270/262904.html

compliance requirements and some cease doing business. The proposed amendments are unlikely to raise these issues they do change the small businesses exemption in the Privacy Act.

Industry group respondents to the targeted consultation process noted there could be some positive and negative impacts on competition as a result of a mandatory scheme. For example, customers may choose to 'vote with their feet' given the likely increased publicity around data breaches or lack of breaches, potentially impacting positively on competition.

Another industry group noted that both general and specific competition issues would arise in the marketing and advertising industry. That group commented that, in general, data-driven marketing and advertising will be less competitive than alternate channels and platforms (such as mass marketing and advertising in traditional broadcast mediums and in print), if the costs of mandatory data breach notification results in a considerable increase in the price of data-driven marketing campaigns. As a result, a mandatory data breach notification scheme would affect the most innovative companies working in Australia's digital economy.

Industry groups also commented that there was the potential for serious and costly reputational damage if the Commissioner directed an entity to notify a general form of notification (eg publication in a newspaper) rather than a targeted notification. A general form would bring exposure to a wider range of the public, including those that are not affected by the data breach. To safeguard against such an outcome, it is expected that the Commissioner's discretion to require notification will be subject to detailed guidance, which would be developed in consultation with relevant stakeholders, including private sector organisations. The Commissioner's discretion will also be subject to merits review by the Administrative Appeals Tribunal.

Finally, an additional competition issue identified was the creation of a higher cost of entry to market. These businesses would be in a similar state to start-up entities, and would need to factor in the costs associated with the creation of a mandatory data breach notification scheme. Although, it is arguable that these are likely to be minor compared with other privacy obligations that will need to be adhered to once a new business starts and becomes subject to the Privacy Act.

Costs impact for business if commencement delayed

Some industry group respondents to the targeted consultation process noted that there would be some alleviation of the costs burden if commencement of the proposed mandatory scheme was delayed beyond March 2014. This was on the basis that industry should be given the time to embed changes into systems and practices for the legislated March 2014 reforms, before considering the need for additional changes to any new regulation.

Other industry group respondents advised that no cost benefit would accrue by delaying the proposals. One group noted that it would be more efficient from a cost perspective to align with the March 2014 compliance date, as particular entities can more easily incorporate these requirements into their implementation processes underway relating to the new APPs and credit reporting provisions.

Similarly, a privacy advocate group commented that the costs for the private sector associated with the implementation of the proposed scheme may be higher if the commencement is delayed beyond March 2014, as there are potential efficiencies to be gained for organisations in dealing with both sets of regulations concurrently.

On the basis of responses to the targeted consultation process, the weight of opinion favoured concurrent commencement of the proposed scheme with the privacy reforms in March 2014.

Impact on the OAIC

The impact on the OAIC is likely to be more significant. As the regulator, it will be expected to receive a larger number of notifications, and will have additional powers to utilise in the event that a failure to comply with a data breach obligation requires investigation. It will be expected to issue new guidance on the new provisions and have increased requests from entities that are keen to ensure they comply with the new legislative requirements.

However, as more entities improve privacy practices, and more information about preventing data breaches is available, there may be a longer term decline in the number of notifications reported to the OAIC and affected individuals. Similarly, while entities

may be more cautious in the shorter term and report more instances to the OAIC, that may decline over time as they more fully understand their obligations.

The OAIC will have a significant workload in both the lead up and commencement of the new privacy reforms in March 2014. That may impact on its ability to produce guidance material pre-commencement, and investigation and enforcement work post-commencement.

Option 3

Agencies and private sector organisations under the Privacy Act could be encouraged to consider developing industry codes that provide a self-regulatory framework tailored to particular industry needs. Such codes could be developed under the new Part IIIB of the Privacy Act (to commence in March 2014) which allows for the Privacy Commissioner to approve and register enforceable codes which are developed by entities, on their own initiative or on request from the Commissioner, or by the Commissioner directly.

Impact on business

There could be a number of benefits to a particular industry sector in developing an industry code. First, they could give entities a sense of active ownership of their privacy obligations. Secondly, it may send a positive statement to the community that a particular entity or group of entities are mindful of the privacy concerns of individuals and are pro-active in protecting their privacy rights. A code may also change the culture of an entity or industry by raising awareness of privacy and introducing a compliance regime. It may serve as a guide to privacy regulation by providing entities with a single document that incorporates all its related legislative requirements and written in a way that is applicable to a particular industry. Finally, it may provide clarity, certainty and satisfaction to consumers seeking redress by incorporating privacy complaint handling procedures in a code.

A code-based approach would allow government and industry sectors to examine more carefully how data breach incidents impact directly on their own particular sectors, and tailor a framework that takes into account existing reporting requirements and compliance issues. This would recognise the need for a flexible approach over a one-size-fits-all legislative approach that may be more a burden for particular industries.

Entities subject to the Privacy Act may support the opportunity to create their own code although this would require those entities to set aside resources to meet with industry counterparts to develop a relevant code. For codes developed under the new Part IIIB of the Privacy Act, the OAIC's recent consultation draft on *Guidelines for developing codes*[30] noted that significant resources may need to be allocated to the development and maintenance of a code, including the following matters:

- investigating the need for a code,
- establishing an administrative mechanism responsible for developing the code, such as a code development committee ,
- drafting the code,
- seeking legal or professional advice,
- involving all stakeholders (including consumers) in an effective public consultation,
- establishing a code administrator to oversee the operation of the code,
- maintaining a register of entities bound by the code and information about the code on a website,
- hiring and training support staff for the code administration, and
- financing the development and ongoing administration of the code, including in relation to regularly reporting on, and independent reviews of, the code

It is possible that the costs associated with the development of a code may outweigh the costs of complying with a mandatory data breach notification scheme, particularly if the new model is largely based on the existing voluntary model.

In addition, most respondents to the targeted consultation process believed that there would be no industry sector impacted disproportionately by the mandatory data breach notification scheme. This suggests that there is no significant view that a particular industry sector will need special treatment (ie a specialised code) to ensure that it does not suffer adversely under the proposed scheme.

[30] http://www.oaic.gov.au/news/consultations/code_development/draft_code_development_guidelines.html

If a Part IIIB of the Privacy Act code was developed, it would have to meet equivalent standards that are currently contained in the OAIC guide, otherwise it is unlikely receive the Privacy Commissioner's approval. Given that the mandatory data breach notification scheme is largely based on the existing voluntary model, it is likely that many of the same costs issues identified under Option 2 will be raised.

There is a risk is that there may not be a consensus among industry participants on a final draft code, which would leave personal information without important privacy protections. The small amount of codes developed under the existing Privacy Act to date indicates that the code regulation framework is not a solution for all industry sectors.

Further, given the different range of industries regulated by the Privacy Act, and the different types of personal information being collected, this approach gives rise to the possibility of an inconsistent and fragmented approach being adopted. This raises the risk that a standardised approach to the handling of personal-information will not be achieved, which would be generally inconsistent with the approach to privacy regulation. That may raise confusion amongst consumers, who might be notified about a data breach that has occurred with a particular entity in one industry sector, but not another. Some entities may also be subject to more than one industry code (eg telecommunications providers) and may be required to implement different responses to data breaches that occur depending on which code is applicable.

On the other hand, provided the standards developed under a code did not result in diminished privacy protection rights relative to similar rights in the APPs, and that the OAIC retained a regulatory oversight or advisory role (so that there was community confidence in this approach), this approach could be beneficial to industry sectors.

Impact on OAIC

The impact on the OAIC is likely to be moderate, depending on its level of involvement in developing and approving the code. As the regulator, it will be expected to promote greater awareness of the OAIC guide and receive increased requests from industry bodies seeking assistance in developing a code. If industry codes are successful in encouraging entities to improve privacy practices, there may be a longer term decline in the number of notifications reported to the OAIC and affected individuals.

Impact on individuals

Similar to option one, there is likely to be little change for individual Australians noting that they face existing risks without a mandatory scheme. Unless a code-based approach is more uniformly adopted across a range of industry sectors, there remains a significant risk that they may continue to be kept unaware in the event that their personal information becomes compromised.

Their expectations may be raised that, with the development of codes, entities will increasingly improve their privacy practices, and that complaint mechanisms will be available.

However, if non-Part IIIB codes are developed, individuals will have no guarantee that industries will develop codes that require notification in the event of a data breach, or at least require data breaches to be notified at the standard ('real risk of serious harm') currently reflected in the OAIC guide and recommended by the ALRC. The different requirements that will apply across industry sectors are also likely to raise confusion amongst the general public.

A non-standardised and inconsistent approach is also less likely to provide the necessary information to meet the 'informational objective', which is intended to provide better information to combat data breaches in the future.

Consultation

Discussion paper

On 19 October 2012, a discussion paper was released seeking public comments on whether Australia's privacy laws should include a mandatory data breach notification requirement and, if so, the possible elements of such a requirement. The deadline for comments on the discussion paper was 23 November 2012, although many submissions were received after that date.

The objective of the consultation was to obtain views of relevant stakeholders to the proposition that a mandatory scheme be introduced. In the ALRC's inquiry, there was strong support in favour of introducing a mandatory scheme, although some large private sector organisations were opposed. The consultation sought to confirm whether those views were still current, but also to seek views on the elements of a model even if a stakeholder had expressed initial opposition.

Using the ALRC recommendation as its basis, the discussion paper sought views on whether the existing voluntary reporting system was operating effectively.

The Government received 62 submissions in response to the issues paper. There were 24 submissions either strongly, or conditionally, in support of the introduction of a mandatory reporting scheme. There were 12 submitters who didn't express a definitive view although most of these did not expressly oppose a mandatory scheme. The group supporting a mandatory scheme included Commonwealth and State privacy/information commissioners, privacy and consumer advocates, academics, IT software and security companies, and some individuals.

There were 27 submitters that opposed a mandatory scheme on the grounds that the existing voluntary scheme is operating effectively, and that a mandatory scheme could bring additional compliance obligations. This group comprised private sector industry groups and individual companies in the banking, telecommunications, retail and online industries, and two key government agencies.

Many of these submitters questioned whether a real problem had been demonstrated both in the numbers of data breaches, and in the effectiveness of the existing voluntary OAIC

guidelines. Some queried whether overseas examples used in the discussion paper provided ample evidence for a mandatory scheme. Some believed the Government should first consider the regulatory impact of the measures in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (due to commence on 12 March 2014) before any new significant privacy reforms are to be introduced. An example of this type of commentary was included in the submission from the Law Council of Australia:

> "The introduction of amendments to the Privacy Act contained in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 is likely to bring about a different privacy landscape and we suggest that the effectiveness and consequences (both intended and unintended) of those amendments should be experienced and properly considered before further amendments are made."

In terms of some specific industry sectors, telecommunications companies opposed further regulation in this area, noting that there were existing measures for the telecommunications industry that encouraged the maintenance of adequate security measures and communication with customers in the event of a breach. Advertising organisations also believed the existing system was operating effectively, noting that there were risks for a business's reputation where it did not adhere to high standards of privacy protection or where it had inadequate responses to breaches. The Australian Bankers' Association stated that there was no apparent evidence of a clear and substantial market failure warranting legislative intervention.

Elements of possible model

The discussion paper also sought responses on possible elements of a legislative model. These included: which entities should be subject to the requirement; the types of breaches that should be reported; who should decide on whether to notify; the content of a notification; the time frame for reporting; the penalty for failing to notify; and whether any exceptions should apply.

The vast majority of submitters who commented on the possible design of a mandatory scheme were in favour of the ALRC's recommended trigger for notification, or a variation of that test, ie a test based on a 'real risk of serious harm' to an individual. This would not require entities to report less serious privacy breaches to affected individuals

or the OAIC. To lessen the regulatory burden, some private sector submitters recommended a higher threshold involving more serious breaches and/or a minimum number of individuals who are personally affected (eg 100-1000 people). Some privacy advocates and the Victorian Privacy Commissioner suggested a lower bar, including, in some circumstances, requiring mandatory notification to the OAIC even where it did not appear to pose harm to individuals.

On the issue of the content of the notification, there were a range of views with private sector submitters preferring less detailed information having to be provided, while privacy commissioners/advocates believed more should be included. For example, Telstra believed it should be limited to the fact of the data breach, the information accessed/disclosed and what affected persons could do to minimise the impacts. On the other hand, the NSW Privacy Commissioner believed it should also include more details about the incident, the action that has been taken as a result of the breach and contacts at the agency or organisation.

The draft legislation has addressed concerns of private sector submitters by requiring less detailed information.

Most submitters agreed that there should be no set time frame for notification given the variable factors unique to each data breach, and that some will be more complex and difficult to assess initially. Submitters favoured a number of tests, including requiring notification 'as soon as practicable', 'as soon as is reasonable in the circumstances', or 'without unreasonable delay'. Most submitters also favoured the form of notification to be whatever is appropriate in the circumstances, or in the form the entity usually communicates with the affected person. This has been reflected in the draft legislation.

In terms of whether to include a penalty, most private sector submitters opposed the inclusion of a penalty, or were only agreeable if it included specified exculpatory factors (eg liability wouldn't arise for unintentional failures to notify). Commonwealth and State Information/Privacy Commissioners and privacy/consumer advocacy groups favoured civil penalties with significant penalties to create a deterrent. For example, the OAIC recommended a civil penalty level similar to the equivalent provision in the *Personally Controlled Electronic Health Records Act 2012* (ie 100 penalty units - $17,000).

The draft legislation has addressed concerns of private sector submitters by ensuring that a civil penalty only applies for serious or repeated breaches of mandatory data breach notification requirements.

There was broad consensus on which entities should be subject to the scheme, with most submitters who commented agreeing with the ALRC's view that it should apply to current entities regulated by the Privacy Act. A small number of submitters argued that all businesses that hold personal information should be subject to the scheme, or that, if the Government removed or amended exemptions in the future (eg small businesses, political parties), those entities should also automatically be subject to the scheme.

The draft legislation has reflected these comments by not applying the scheme to small businesses.

Confidential targeted consultation

In April 2013, an Exposure Draft Bill was provided on a confidential basis to a targeted group of stakeholders. The purpose of the consultation was to obtain more information to assist the Government in making a decision about whether to introduce a mandatory data breach notification scheme.

The key features of the Exposure Draft Bill that was provided for comments were:

- the proposed model would create a requirement to notify the OAIC and affected individuals where there has been a data breach which has given rise to a 'real risk of serious harm' to an affected individual. That was the ALRC's recommended approach. A real risk is defined as a risk that is not a remote risk. This would mean entities would not be required to report less serious privacy breaches to affected individuals or the OAIC.
- the requirement to notify would apply to data breaches involving personal information, credit reporting information, credit eligibility information and tax file number information.
- the content requirements of the notification are, at a minimum: a description of the breach; a list of the kinds of personal information concerned; contact information for affected individuals to obtain more information and assistance; and recommendations about the steps that individuals should take in response to the breach.

- the OAIC will have the power to compel notification to affected individuals where it becomes aware of a serious data breach that has not been notified (as a result of an individual's complaint or otherwise) and it is in the public interest to do so; and
- the OAIC would have its normal investigative and enforcement powers in relation to non-compliance with an obligation to notify. Consistent the measures in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, a civil penalty would only be applicable where there has been a serious or repeated non-compliance with mandatory notification requirements.

The targeted group was invited to make any comments on the legislative model. It was also asked to make comments on how the legislative model would impact on the costs that regulated entities might incur as a result of a new legislative requirement. Specifically, the targeted group was invited to comment on the following questions:

(1) What is likely to be the 'paper burden' or administrative costs (quantified if possible) to private sector organisations under the mandatory scheme in the Exposure Draft Bill? In particular, what will be the burden for entities that:

   a. Have existing systems in place to comply to make notifications (where necessary) consistent with the existing voluntary *Data Breach Notification* Guide of the Office of the Australian Information Commissioner?, and

   b. Have no systems in place and may have 'start up' costs?

(2) In your view, will particular industry sectors incur costs disproportionately under the scheme in the Exposure Draft Bill than other regulated entities under the *Privacy Act 1988*?

(3) Will the scheme in the Exposure Draft Bill result in any restrictions on competition?

(4) Will the costs impact on private sector organisations be different if the commencement of the mandatory scheme in the Exposure Draft Bill was delayed beyond 12 March 2014 (ie beyond the date that the key measures in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* commence).

The Government received 9 submissions in response to the issues paper. These came from a range of industry groups representing banks, telecommunications providers, financial service providers, internet companies and direct marketers. Submissions were also received from privacy and consumer advocates. Detailed discussion and analysis of the responses to this consultation process have been included in the ''Impact Analysis' section above.

Conclusion

In this RIS, three options have been considered:

- Option One: Maintaining the status quo; or
- Option Two: Introduce a mandatory data breach notification scheme.
- Option Three: Encourage industry to develop industry codes.

The preferred option is Option Two.

Option Two would require the introduction of a legislative requirement which would have impacts on individuals, businesses, and the OAIC.

Option Two would provide individuals with the information that a breach of their personal information has occurred. Concerns about the safety and security of personal information in the online environment have been identified as key issues for individuals. Individuals could be in a position to take steps to mitigate against the possibility of identity theft or fraud, which might cause them financial loss. This will be an important measure to assist in combatting cybercrime, which is consistent with US studies which indicate mandatory data breach notification laws have an effect in lowering identity theft rates,. On the other hand, a mandatory notification scheme may provide little or no relief for some individuals whose health information has been published online and made widely known before being removed.

As noted in the analysis, there will be cost impacts on businesses. The Privacy Act applies to private sector organisations that have a turnover of more than $3 million, and to some small businesses which are subject to the Privacy Act (eg those that trade in personal information). A number of administrative costs have been identified by industry groups such as creating notification methods, formalising internal processes and increased insurance and legal costs. To address concerns of those who identified particular administrative costs to the business, the Bill has been amended to make the means of notification more flexible.

However, specific costs estimates varied from a small group of stakeholders who believed there would be large costs amounts to most who believed there would be modest cost implications. Privacy and consumer advocates believed costs would be

minimal, and should be considered necessary where an entity handled personal information. More detailed US studies indicate that the notification cost component of addressing a data breach was on the increase.

There are a range of views about whether particular industry sectors would incur costs disproportionately under a mandatory scheme. While most believe there would no disproportionate impact, some identified small businesses (eg those that trade in personal information) and financial services sector businesses as entities that may incur adverse impacts more than other businesses.

Option Two would create positive and negative impacts on competition. Consumers could be more likely to move to competitor companies with better security, or response measures, to data breaches. There may be particular adverse competition implications within the data-driven marketing and advertising industry for smaller operators within that industry, and data-drive marketing campaigns launched on behalf of other businesses. The power for the Commissioner to direct that a mandatory data breach notification occur could also expose a business and its data breach to a wider audience, thereby causing more reputational damage than a normal notification from a business to its affected customers.

A possible delay in the commencement of the introduction of a mandatory data breach notification scheme could alleviate the costs burden for businesses, although it could also be more efficient if it is aligned with major privacy reforms that will commence in March 2014. On the basis of the analysis in the RIS, Option Two would be the most effective option to safeguard the personal information of individuals and encourage improvements in privacy practices, although it will raise cost impacts for businesses which will be subject to the scheme, and resource implications for the OAIC, which will have regulator functions relating to the scheme.

.

Implementation and review

Any reforms would be implemented through amendments to the *Privacy Act 1988*. It is anticipated that the amendments will form part of a Bill to be introduced in the 2013 Winter Sittings. It is proposed that the amendments commence at the same time as key amendments in the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which is 12 March 2014. The amendments will apply prospectively to data breaches that occur after 12 March 2014.

To review the effectiveness of the changes it is proposed that these measures be included in a review to be undertaken 12 months after commencement of the major privacy reforms in March 2014, which were contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. A 12 month post commencement review was a recommendation of the House of Representatives Standing Committee on Social Policy and Legal Affairs, which was accepted by the Government. The review would include an assessment of the impact of the proposal and its effectiveness in meeting its objectives and the actual costs to stakeholders of the implementation of the reforms.

In the lead up to commencement of the amendments, it would be expected that the OAIC will develop and publish guidance about the operation of the new scheme. This may be in the form of a modified OAIC guide on data breach notification, and provide guidance about the practical aspects of the scheme. It would be expected that the OAIC will undertake consultation as necessary with stakeholders, including private sector organisations, in the development of that guidance.

Attachment A

Australian Law Reform Commission recommendation 51-1

Recommendation 51-1 The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:

(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

(b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number.

(c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:

(i) whether the personal information was encrypted adequately; and

(ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the *Privacy Act* (provided that the personal information is not used or subject to further unauthorised disclosure).

(d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.

(e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.