Australian Government
Attorney-General's Department

Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

Regulation Impact Statement

Contents

Background

Australian Law Reform Commission Report on Privacy

In May 2008, the Australian Law Reform Commission (**ALRC**) 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]. The ALRC's report, *For Your Information: Australian Privacy Law and Practice* (**ALRC report**), 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 responded to the majority of these recommendations with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which introduced major privacy reforms and commenced in March 2014.

One of the ALRC's other recommendations was that a mandatory data breach notification scheme be introduced (rec 51-1). Submissions to the ALRC's inquiry indicated strong support for the introduction of a mandatory notification requirement, although some key private sector organisations in the banking and telecommunications industries were not supportive[2].

The ALRC noted developments in international jurisdictions where legislative reform has been implemented. In particular, the ALRC considered that the United States, where at the time mandatory data breach notification was required in more than 30 states, was at the 'forefront in the development of such laws'[3].

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 jurisdictions (i.e. a test based on a real risk of serious harm to an affected individual following a data breach, rather than a test that is satisfied whenever a data breach occurs). Amongst other things, the ALRC believed that a higher threshold for notification should also reduce the compliance burden on agencies and organisations.

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 national privacy regulator (currently the Office of the Australian Information Commissioner (**OAIC**)) 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 notification requirements.

Government response to the ALRC Report

On 14 October 2009, the Government released a First Stage Response to the ALRC report, which addressed 197 of the Commission's 295 recommendations. Recommendation 51-1 was not part of the 197

[1] See *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)* on the Australian Law Reform Commission website.
[2] ALRC Report, paragraphs 51.52 – 51.56.
[3] ALRC Report, paragraphs 51.3 and 51.14.

recommendations and was identified along with a number of other recommendations as requiring consultation and consideration.

International trends since the ALRC Report

Since the ALRC Report, the trend in international jurisdictions has been towards the development and implementation of legislative requirements for notification of data breaches. Forty-seven US states have implemented mandatory data breach notification, and in January 2015, President Barack Obama proposed a national data breach notification standard in the draft *Personal Data Notification & Protection Act*. The proposed scheme would require notification if there is any reasonable risk of harm or fraud to individuals following a data breach.

Elsewhere, the European Union has introduced regulations that mandate data breach notification. In May 2014, New Zealand announced plans to introduce a two-tier mandatory data breach notification scheme. On 16 June 2015, Canada passed legislation to introduce a national mandatory data breach notification scheme.

Voluntary data breach notification scheme

In 2008 the then Office of the Privacy Commissioner (**OPC**) released *Data breach notification — A guide to handling personal information security breaches* (**Data Breach Guide**) in response to requests for advice from agencies and organisations about data breaches, and in recognition of the global trends relating to data breach notification.[4] The Data Breach Guide encouraged entities to voluntarily notify the Privacy Commissioner of data breaches that satisfied the ALRC's recommended 'real risk of serious harm' test, and provided guidance about how to identify and contain a data breach.

The OAIC, which replaced the OPC as the national privacy regulator in November 2010, revised the Data Breach Guide in 2011 and 2014 to reflect changing attitudes and approaches to data breach management, and amendments to the Privacy Act.

The table below captures the number of voluntary data breach notifications made to the OPC/OAIC since 2009-10, when figures about the number of voluntary notifications were first reported separately from the total number of Privacy Commissioner investigations conducted. The number of notifications in 2014-15 was 250% higher than in 2009-10, possibly reflecting increased awareness of privacy obligations among entities following the passage of the *Privacy Amendment (Enhancing Privacy Protection) Act in November 2012*, and the extensive amendments to the Privacy Act that occurred upon its commencement in March 2014.

Year	**Voluntary data breaches to the privacy regulator**
2009-10	44
2010-11	56
2011-12	46

[4] See the current version of the Data Breach Guide on the Office of the Australian Information Commissioner website.

Year	Voluntary data breaches to the privacy regulator
2012-13	61
2013-14	71
2014-15	110

Consultation in 2012 and 2013

2012 Discussion Paper on a mandatory data breach notification scheme

On 19 October 2012, the Government released a Discussion Paper (**2012 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 2012 Discussion Paper and the responses to it are outlined and analysed in more detail below.

Further 2013 targeted consultation

In April 2013, the Government undertook confidential targeted consultation (**2013 targeted consultation**) on a more detailed legislative model. This consultation process invited comments on the legislative model that would form the basis of the *Privacy Amendment (Privacy Alerts) Bill 2013* (**Privacy Alerts Bill**). The consultation sought particular views on the possible costs to business.

Privacy Alerts Bill

On 29 May 2013, the then Government introduced the Privacy Alerts Bill into the House of Representatives. If passed, the Privacy Alerts Bill would have introduced the requirement to notify the OAIC and affected individuals where there has been a data breach which gives rise to a 'real risk of serious harm' to an affected individual.

The Privacy Alerts Bill was intended to implement ALRC recommendation 51-1 and strengthen the existing voluntary data breach notification framework in order to counter underreporting of data breaches and to help prevent or reduce the effects of serious crimes like identity theft. The 2013 Bill was based on the general requirements of Australian Privacy Principle (**APP**) 11 in the Privacy Act, which requires regulated entities that hold personal information to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. (Sections 20Q and 21T of the Privacy Act impose equivalent obligations on credit reporting bodies and credit providers. Similarly, section *11(1) of the statutory Privacy (Tax File Number) Rule 2015* requires tax file number (**TFN**) recipients to protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure.)

On 6 June 2013, the House of Representatives passed the Privacy Alerts Bill with bipartisan support.
On 17 June 2013, the Bill was introduced into the Senate and was referred on 18 June 2013 to the Legal and Constitutional Affairs Legislation Committee for inquiry. The committee reported on 24 June 2013, its sole recommendation being that the Senate pass the Privacy Alerts Bill. The Privacy Alerts Bill lapsed on prorogation of the 43rd Parliament.

Parliamentary Joint Committee on Intelligence and Security Reports

2013 Report

In May 2012, the then Government asked the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) to inquire into a package of potential reforms to Australia's national security legislation including a mandatory data retention regime for personal telecommunications data. The PJCIS reported a large number of the submissions to the inquiry objecting to data retention on information security grounds, including concerns about creating a 'honeypot' of information that would be vulnerable to a data breach[5].

In May 2013, the PJCIS released *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The report recommended that, if a mandatory data retention regime should proceed, its introduction should include the introduction of a robust mandatory data breach notification scheme (Recommendation 42).

The Commonwealth Attorney-General's Department submitted to the inquiry that, if enacted, mandatory data breach notification laws could complement the current legislative security requirements and a data retention regime in a least four ways, by:

1. mitigating the consequences of a breach;
2. creating incentives to improve security;
3. tracking incidents and providing information in the public interest; and
4. maintaining community confidence in legislative privacy laws[6].

2015 Report

In November 2014, the Government referred the provisions of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (**Data Retention Bill**) to the PJCIS for inquiry and report. The PJCIS considered evidence provided by the Privacy Commissioner and others that, by creating a large repository of personal information, the proposed data retention scheme increases the risk and possible consequences of a data breach and that a mandatory data breach notification scheme is one way to manage the impact of any data breach on individuals[7].

In February 2015, the PJCIS released the *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. The report recommended the introduction of a mandatory data breach notification scheme by the end of 2015 (Recommendation 38). On 3 March 2015, the Government agreed to all recommendations of the report, including the introduction a mandatory data breach notification scheme. The Government stated it would consult on the draft legislation for the mandatory data breach notification scheme.

---

[5] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 2013, pages 167-75.
[6] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 2013, pages 175.
[7] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 2015, pages 293-5.

What is the problem trying to be solved?

What a data breach is

Under the OAIC Data Breach Guide, a data breach is defined as the situation where 'personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference'[8]. The ALRC report noted that, with advances in technology, entities are 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 result from the unauthorised release or loss of information held by an agency or organisation. Currently, there is no mandatory requirement that an entity inform an individual following a data breach involving their personal information.

The OAIC Data Breach 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 Data Breach 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[9].

Why data breaches are a problem

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 details about individuals' personal preferences and occupational history is increasingly transitioning to web pages and data centres, with varying degrees of accessibility and security.

APP 11 in the Privacy Act requires organisations that hold personal information to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. However,

[8] Data Breach Guide, page 2.
[9] Data Breach Guide, page 5.

organisations have no legal obligation to notify an individual if their personal information is breached (with the exception of eHealth information as discussed below). This is regardless of the sensitivity of the personal information and regardless of the risk of harm that may arise from the data breach.

The absence of a requirement to notify individuals of serious breaches involving personal information does not align with the almost universal agreement from the Australian public that an organisation should inform them if their personal information is lost[10].

The Data Breach Guide promotes the notification of serious data breaches. However, it is voluntary. A key issue is whether the Data Breach Guide is operating as an effective means to encourage widespread notification of breaches. As numbers cited above demonstrate, voluntary notifications have increased by 250% since 2009-10, from 44 to 110. However, the OAIC predicts, based on comparisons with other jurisdictions, that notifications under a mandatory scheme would nearly double to around 200.

Another issue with a voluntary scheme is potential inconsistency in how entities choose to participate. An example is a recently concluded Privacy Commissioner investigation where an entity voluntarily notified a data breach three years after it occurred[11]. Although the Commissioner expressed concern about the significant delay between when the entity became aware of the data breach and when it chose to notify the breach, the Commissioner's current investigative and enforcement powers are based around requirements of the Privacy Act, and are not designed to deal with cases where a business's voluntary data breach notification practices possibly do not reflect community expectations.

This supports a conclusion that a continuation of voluntary data breach reporting will contribute to the extent of the data breach problem.

Identity crime

Any breach of the secure storage of personal information an entity holds may be sufficient to allow an unauthorised person to assume the identity of the victim and use that illicit identity to open, for example, new accounts in the victim's name. A stolen identity can be used to commit identity fraud where a fabricated, manipulated or stolen identity is used to gain a benefit or avoid an obligation[12].

A report released in 2014 indicated data breaches, whether accidental or deliberate, present significant opportunities for obtaining personal identifiable information that is used in identity crime. The types of personal information used to commit identity crime are increasingly being collected and stored in databases held by a variety of government agencies and private sector organisations and the aggregation of this information, particularly in electronic forms that are accessible online, increases the risk that information may be acquired through data breaches, either accidentally or through deliberate attempts to steal personal information[13].

[10] *Community Attitudes to Privacy survey Research Report 2013*, Office of the Australian Information Commissioner, 2013 (Community Attitudes Report), page 5.
[11] See Statements on the Office of the Australian Information Commissioner website.
[12] ALRC Report, paragraph 51.4.
[13] *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot.,* Attorney-General's Department, 2014, page 23.

Under the voluntary system, the notification of individuals can be delayed for years, as discussed above. Such a failure to notify an affected individual of a data breach in a timely manner increases the potential cost of the data breach on the individual. For example, a delay in notification increases the risk of an affected individual becoming a victim of an identity crime such as identity theft, as they may be unaware of the need to mitigate against the data breach.

The magnitude of data breaches

Studies and anecdotal evidence suggest that breaches of data security are increasing in frequency and scope. There have been a number of recent high profile data breaches that have highlighted the magnitude of the issue. Examples in Australia and abroad include:

a. In October 2013, Adobe reported that it had been the target of a cyber–attack that affected at least 38 million Adobe customers globally, including over 1.7 million Australians.[14]
b. In June 2014, Optus reported 3 separate data breaches where the security of the personal information of over 300,000 of its customers was compromised[15].
c. In February 2014, a data breach at the Commonwealth Department of Immigration and Border Protection compromised the personal information of approximately 10,000 asylum seekers[16].
d. In November 2014, a hacking incident at Sony Pictures Entertainment was discovered that involved the personal information of employees, including social security and health information, as well as other Sony corporate information[17].
e. In June 2015, the Privacy Commissioner finalised enquiries into a data breach of Australian online retailer Catch of the Day, expressing concern that the data breach, which occurred in May 2011, had not been notified to the Commissioner until June 2014[18]
f. In July 2015, the US Office of Personnel Management outlined details of two data breaches that compromised personal information about more than 21.5 million current and former US Government employees and other individuals[19].
g. In July 2015, client data from dating website Ashley Madison was stolen and published online in August 2015. Media reports about the number of affected Australians range from 460,000–900,000. The Acting Australian Information Commissioner announced an investigation into the data breach on 25 August 2015[20].
h. In September-October 2015, retailers Kmart and David Jones disclosed that their online stores experienced data breaches compromising names, email and postal addresses and order details of some customers. Both retailers publicly announced the breaches, voluntarily notified the AFP, the OAIC and affected individuals, and engaged expert IT security advice. In

[14] See Commissioner initiated investigation reports on the Office of the Australian Information Commissioner website.
[15] See at Singtel Optus: enforceable undertaking on the Office of the Australian Information Commissioner website.
[16] *Department of Immigration and Border Protection: Own motion investigation report [2014]* AICmrCN 5 (12 November 2014).
[17] See Sony Pictures Entertainment's notification to affected individuals (made in accordance with Californian mandatory data breach legislation) on the Office of the Attorney General website.
[18] See Statements on the Office of the Australian Information Commissioner.
[19] See OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats on the Office of Personnel Management website.
[20] See Statements on the Office of the Australian Information Commissioner.

both cases the OAIC stated it would await further information from the retailers and praising the voluntary notification of the breaches[21].

There are numerous reports providing details of the magnitude and costs of data breaches and the linked issue of identity crime. One 2015 report that collected data breach information from 70 organisations in 61 countries identified 79,790 security incidents and 2122 confirmed data breaches. It reported an overall cost of $400 million from the 700 million compromised records[22]. Another global report identified 312 breaches, with 348 million identities exposed, with an average of 1.1 million average identities exposed per breach[23]. A recent report estimated that $US16 billion was stolen from 12.7 million identity fraud victims in the U.S in 2014[24].

Who data breaches affect

The impact of data breaches and related identity crime is widespread and affects government agencies, non-government entities and individuals. A 2015 report specific to Australia commissioned by IBM and conducted by the Ponemon Institute assessed the cost of 23 government and non-government data breaches and found the average total cost of a data breach to business was $2.82 million with a cost of $144 per lost or stolen record[25]. It appears that a considerable proportion of data breaches involve the loss or theft of personal information that is ultimately used in identity crime. A recent US study found that two-thirds of identity fraud victims in 2014 had previously received a data breach notification in the same year[26].

Identity crime is one of the most prevalent types of crime affecting Australians. A 2013 Australian Institute of Criminology survey found the economic impact of identity crime to Australia is likely to exceed $1.6 billion dollars every year. It found 9.4 percent of people reported having their personal information stolen or misused in the previous 12 months, with five percent reporting that they suffered financial losses as a result[27]. On average, victims of identity crime lose $4,101 per incident and spend at least 8 hours dealing with the consequences of the incident. The survey found with 15 percent of victims experienced mental or physical health impacts that led them to seek counselling or other medical treatment.

Community expectations

According to a 2013 national privacy survey conducted by the OAIC, the security of personal information, particularly on the internet, concerns the majority of Australians[28]. Eighty-nine per cent of respondents worried about the security of their personal information when using the internet, 69% did not trust social

[21] See at: http://www.oaic.gov.au/news-and-events/statements/privacy-statements/kmart-australia-data-breach/, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/david-jones-data-breach/.
[22] *2015 Data Breach Investigations Report*, Verizon (Verizon Report), page 1.
[23] Symantec Report, pages 78-81.
[24] *2015 Identity Fraud: Protecting Vulnerable Populations*, Javelin Strategy & Research, 2015.
[25] Ponemon Institute, *2015 Cost of Data Breach Study: Australia* (Ponemon Report), page 1.
[26] *2015 Identity Fraud: Protecting Vulnerable Populations*, Javelin Strategy & Research, 2015.
[27] *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot*, Attorney-General's Department, 2014.
[28] *Community Attitudes to Privacy survey Research Report 2013*, Office of the Australian Information Commissioner, 2013 (Community Attitudes Report), pages 3-5.

media services to protect their information and, 8% avoided using credit cards online due to concerns about the security of their personal information.

The survey also found that two-thirds of Australians are concerned that they may become a victim of identity theft and fraud in the next year, and one third say that they have had problems with the way that their personal information was handled in the previous year. The survey identified that over 90% of the Australian public thinks that both government and private business organisations should inform them if their personal information is lost and how they protect and handle personal information in the first place.

Current data breach requirements

My Health Records

At present in Australia, mandatory data breach notification requirements apply only in the event of unauthorised access to certain eHealth information under the *My Health Records Act 2012* (**MHR Act**). Under the MHR Act, certain participants (the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider) are required to report data breaches that occur in relation to the eHealth record system to the OAIC and the System Operator. Failure to report a data breach could be a breach of the MHR Act, and penalties may apply.

Voluntary data breach notification scheme

In the absence of a legal requirement, entities are encouraged to adhere to the OAIC Data Breach Guide. The Data Breach Guide outlines key steps and factors agencies and organisations should consider when responding to a data breach involving personal information that they hold. The Data Breach Guide provides advice around 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 misuse, interference and loss, and from unauthorised access, modification or disclosure. 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. undertake notification (if appropriate); and
4. prevent future breaches.

Why is government action needed?

APP 11 of the Privacy Act obliges regulated entities to take reasonable steps to maintain the security of the personal information they hold, while other provisions create equivalent obligations in regard to other kinds of information. However, the Privacy Act does not oblige entities to notify individuals whose personal or other information has been compromised. Entities that do not participate in the voluntary scheme face no legal sanction.

The OAIC's view is that notification may be a 'reasonable step' where a data breach has occurred (with 'reasonable step' being a key term used in APP 11 and other Privacy Act security provisions mentioned

above). 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.

The Privacy Act's information 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.

The Privacy Commissioner has publicly stated that, based on media reports citing information technology security experts, the OAIC has likely only been notified of a small percentage of data breaches that are occurring[29]. In its submission to the 2012 Discussion Paper, the Centre for Internet Safety also asserted that significant amounts of underreporting had been occurring.

On the other hand, some respondents to the 2012 Discussion Paper 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 2012 Discussion Paper revealed that attempting to quantify the problem is difficult because many organisations do not have the capability to detect whether data loss has occurred, and whether there has been a significant impact or harm caused by such data loss.

Does the Government have the capacity to successfully intervene?

In terms of whether a mandatory notification scheme would operate to limit the harmful effects of a data breach, some private sector stakeholders in responses to the 2012 Discussion Paper and in the 2013 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 2013 targeted consultation process.

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%[30]. It is therefore open for the conclusion to be drawn that data breach laws are a longer term effective measure in combating identity theft.

---

[29] See, for example, at: http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/inquiry-into-privacy-amendment-privacy-alerts-bill-2013 and http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/the-importance-of-information-security-in-protecting-privacy.

[30] 'Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated)', Sasha Romanosky, Rahul Telang and Alessandro Acquisti, *Journal of Policy Analysis and Management*, Vol. 30, No. 2, pp. 256-286, 2011.

It is difficult to determine whether or to what extent mandatory data breach notification would produce similar results in Australia. However, if introduction curbed identity theft to the same extent as the US study results in the long term, the Australian Institute of Criminology figures cited above suggest savings of $AUD96.7 million per annum.

What is the alternative to Government action?

The alternative to government action is the maintenance of the current voluntary data breach notification scheme and its associated under-reporting of data breaches to individuals to whom the personal information breached relates. This alternative to action could see the costs of data breaches to organisations, government and individuals continuing to increase.

The *2015 Cost of Data Breach Study: Australia* reports the costs to businesses of data breaches have increased from $123 per compromised record in 2010 to $144 per compromised record in 2015 amounting to a total organisational cost of data breaches rising from $1.97 million in 2010 to $2.82 million in 2014. The cost associated with the business losses from data breach, such as abnormal turnover of customers, reputation losses and diminished goodwill, increased from $0.66 million in 2010 to $0.89 million in 2015[31].

What are the objectives of Government action?

The objectives of the Privacy Act accord with the objectives of a mandatory data breach notification scheme. The objective of the Privacy Act is 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.

The ALRC Report stated that the key objective of mandatory data breach notification is to allow individuals whose personal information had been compromised in a data 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 monitoring their accounts or taking preventative measures such as changing passwords and cancelling credit cards.

A mandatory scheme would also encourage agencies and organisations to be transparent about their information-handling practices. This would support the operation of existing APP 1 in the Privacy Act, which requires entities to make available a clearly expressed and up-to-date policy about how the entity manages personal information.

A mandatory scheme would also likely 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 a reason why some private sector organisations do not notify regulators or affected individuals about data breaches.

Evidence suggests this concern is valid to some extent: a 2015 Deloitte survey conducted in Australia found that 27% of survey respondents who had received a voluntary data breach notification trusted the notifying

[31] Ponemon report.

entity less. Importantly, however, these respondents were outweighed by the 34% of respondents who actually trusted the entity more, presumably because of the transparency shown in undertaking notification[32]. Given the figures from the OAIC's 2013 national privacy survey cited above showing strong community support for data breach notification, the potential loss of trust following a notification would also need to be balanced against the possible reputational risk of not notifying a data breach that later comes to light.

Nonetheless, the Ponemon Report found that the rate of customers terminating their relationship with companies following a data breach was increasing. The same report found that the cost of a data breach is lower for companies that have strong information security policies in place before a data breach occurs[33].

In its submission to the 2012 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. Among other things, mandatory data breach notification will provide the OAIC with information about trends in data breaches that may assist in the development of useful guidance material for entities about information security.

What policy options are being considered?

Option One – Retain the status quo

Option One 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 except in relation to the MHR Act. They will continue to be obliged under the Privacy Act to secure personal and other specific kinds of information they hold, and will continue to be encouraged to comply with the existing OAIC Data Breach Guide.

The Data Breach Guide will continue to provide 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. Entities will also be able to draw on other relevant OAIC guidance material, such as the APP

[32] *Deloitte Australian Privacy Index 2015: Transparency is opportunity*, Deloitte, 2015 (Deloitte report), page 11.
[33] Ponemon report, page 2.

Guidelines[34], which provide advice about key terms in the Privacy Act, as well as compliance with APP 11, and the *Guide to Securing Personal Information*[35], which provides advice about 'reasonable' information security steps under the Privacy Act. This guidance material expresses the view that, depending on the circumstances, 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 2012 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 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 Privacy Commissioner where appropriate and in dealing with the privacy concerns of their customers. They also argued that, contrary to anecdotal reports, there is no real evidence in Australia of underreporting of significant data breaches to the OAIC. Additionally, some argued 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[36].

The Information Commissioner has an existing power under the Privacy Act to audit private sector organisations which could be used to investigate actual or suspected data breaches (for example, following complaints from affected individuals, media articles or other information). This has the potential to make it more difficult for an entity to hide a data breach. For reputational risk reasons, the possibility of being audited provides the incentive to report data breaches to the Commissioner and affected individuals proactively.

Option Two – Introduce a scheme for mandatory notification of serious data breaches

Option Two is to amend the Privacy Act to require entities to report serious data breaches to the OAIC and to affected individuals. A serious data breach is one that gives rise to a real risk of serious harm to any of the individuals to whom the information relates. Option Two will make no changes to the mandatory scheme operating under the MHR Act.

[34] See APP guidelines on the Office of the Australian Information Commissioner website.
[35] See Guide to securing personal information on the Office of the Australian Information Commissioner.
[36] *Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment*, Centre for Internet Safety, 2012, page 1.

Who would the option apply to?

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 2012 Discussion Paper. This would not include entities, or some of their activities, that fall within exemptions in the Privacy Act, such as political parties, media organisations and most small businesses.

Notification threshold

Under the proposal, a serious data breach occurs following unauthorised access to or disclosure of, or loss of, personal or other specific kinds of information about an individual, where there is a *real risk of serious harm* as a result. This 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.

In the 2013 targeted consultation support was expressed for more explanation about, or a definition of what constitutes '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 that could lead to notification fatigue and create resourcing issues at the OAIC. To address this concern, the proposed model:

a. provides an expanded definition of 'harm' compared to the 2013 proposal;
b. provides a list of matters to be regarded when determining whether there is a real risk of serious harm to an individual (for example, the entity could consider whether information compromised in a data breach was encrypted, or whether the entity has taken steps to reduce the risk of harm so that it no longer meets the threshold); and
c. explicitly provides that, where an entity is unsure whether a serious data breach has occurred, the entity has time to assess whether a serious data breach has occurred, with no further action required if the assessment finds that no serious data breach occurred.

The notification threshold in Option Two is a high one compared to mandatory data breach notification schemes in other jurisdictions: for example, European Union regulations mandate notification following any data breach involving personal information, regardless of whether there is any level of risk to affected individuals; Californian legislation requires notification following any breach of unencrypted personal information, regardless of the risk to individuals; while proposed United States federal legislation would require notification if there is any reasonable risk of harm or fraud to individuals following a data breach. The only jurisdiction with a comparable notification threshold is Canada, which has introduced a mandatory data breach notification scheme which compels an organisation to notify an individual of any breach of security safeguards involving the individual's personal information under the organisation's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

The notification requirement under Option Two 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. Consistent with ALRC recommendation 51-1, under Option Two it would also be possible to prescribe in regulation further specific kinds of information (for example, specific government identifiers) where unauthorised access or disclosure, or loss, is automatically considered to be a serious data breach.

Who must make the notification?

The ALRC recommended that the entity involved in the breach should have the responsibility of notification. Most respondents to the 2012 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. Option Two incorporates this approach.

Option Two would also allow the OAIC to direct an entity to notify a serious data breach. This power is primarily intended to operate in cases where an entity fails to comply with the mandatory notification requirement of its own volition. 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'. An entity would be able to seek review, at the Administrative Appeals Tribunal, of an OAIC decision to issue a direction.

Content of notification

The ALRC report 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.

Option Two incorporates these suggestions and also requires recommendations about the steps that individuals should take in response to the serious data breach. These are based on the existing OAIC voluntary standards.

Where the Information Commissioner directs an entity to notify a serious data breach, the Commissioner would also have discretion to direct the entity to include other information about the serious data breach in the notification. This reflects that the power to compel notification is intended to be used where an entity has failed to voluntarily notify a serious data breach, in which case it may be appropriate in some cases to include additional information in the notification (such as information about complaint mechanisms available under the Privacy Act).

Means of notification

During consultation in 2012 and 2013 there was general support from stakeholders that the means of notification should be directly by phone, letter, email, in person, or by normal means of communication between the entity and the individual. In the 2013 targeted consultation, industry groups expressed the wish for flexibility so that regulated entities could notify individuals in a variety of ways.

Option Two incorporates a flexible approach to notification as it provides entities with the ability to notify an affected individual using the methods of communication it would normally use to contact the individual. Where there is no normal mode of communication with the particular individual, the entity must take reasonable steps to communicate with them. Reasonable steps could include making contact by email, telephone or post.

Furthermore, should it be impossible or impracticable for the entity to notify each individual, the proposal does not require direct notification but rather requires the entity to publish the notification on its website (if any), and to take reasonable steps to publicise the notification. This will ensure that entities are not required to notify each affected individual if, for example, it would be impracticably expensive to do so. It also

recognises that different kinds of notification techniques will be appropriate for different kinds of entities and data breaches (for example, it may be reasonable for some entities to publish information about a serious data breach via social media, whereas for others a newspaper advertisement may be reasonable).

When is notification required?

Option Two also provides that an entity should be required to notify as soon as practicable after it becomes aware or ought reasonably to have become aware of a serious data breach. This accords with the consensus amongst submitters to the 2012 and 2013 consultations who believed that flexibility, rather than a set time frame, was needed given the variable factors unique to each data breach. Where an entity is unsure of whether a serious data breach has occurred, Option Two also explicitly provides the entity with time to investigate the circumstances of the incident to determine whether notification is required (with no further action required if the notification threshold has not been met).

Option Two enables the Information 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.

Failure to notify

The Commissioner's power to direct an entity to notify a serious data breach is expected to be the most likely first regulatory response in the event that an entity fails to comply with its mandatory notification obligations.

Option Two would also link into the existing penalty structure in the Privacy Act, where (should the direction power prove inadequate, or where a further regulatory response is appropriate) less severe sanctions could be used before elevating to a civil penalty. These less severe penalties could follow a 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 Three 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 Data Breach Guide. This proposal would be assisted by OAIC guidance material, specifically its *Guidelines for Developing Codes* (**Code Guidelines**). Some industry groups have developed self-regulatory codes as a tool to promote standard practices and compliance.

The Ponemon Report (while acknowledging a small sample size) indicates that the per capita cost of data breach incidents is different for particular industries, with financial services, industrial and energy companies incurring higher costs[37]. This finding is borne out in a separate 2015 Ponemon Report analysing worldwide data breach trends, though Ponemon found that healthcare and education entities experienced the highest

[37] Ponemon Report, page 2.

data breach costs internationally[38]. Findings such as these 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 2013 targeted consultation process. Some believed that there would be no disproportionate adverse impact on different industry groups, while others believed that small businesses (i.e. those subject to the Privacy Act because they trade in personal information, or are health service providers) would be affected in that way.

Under Part IIIB of the Privacy Act, the Information Commissioner can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Commissioner, or developed by the Commissioner directly. An entity (or a body or association representing them) can develop a written code of practice for the handling of personal information that sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code.

An entity bound by a registered code must not do an act, or engage in a practice, that breaches that code and a breach of a registered code will be an interference with the privacy of an individual under the Privacy Act and subject to investigation by the Information Commissioner. While the Privacy Act allows the development of codes which would allow particular industries to develop a more tailored approach to personal information-handling, these cannot derogate from minimum standards set out in the APPs.

Option Three would 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. Furthermore, the OAIC's *Guide to Securing Personal Information* and *Privacy Management Framework: Enabling Compliance and Encouraging Good Practice* contains suggested standardised rules that may help industry to adopt a self-regulatory framework.

What is the likely net benefit of each option?

Option One — Retain the status quo

Who would be affected

Business

Businesses would continue to have the option to notify when data breaches occur and utilise the OAIC Data Breach Guide.

Individuals

The notification of individuals whose personal information is the subject of a data breach will continue to occur if an APP entity voluntarily undertakes notification.

[38] *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, 2015, page 2.

Government

Government agencies would continue to have the option to voluntarily notify individuals if there has been a breach of the individual's personal information. If agencies choose to notify individuals they would be able to use the OAIC Data Breach Guide to inform their approach.

The OAIC would continue to provide guidance for the management of data breaches in the Data Breach Guide and other related guidance material.

Net benefit analysis

Option One is unlikely to have any additional effect. Agencies and private sector organisations under the Privacy Act will continue to operate in accordance with the APPs, and be encouraged to continue to report significant data breaches to the OAIC and affected individuals. 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 Data Breach Guide.

Under this option, there is likely to be little impact on the OAIC, who will continue to acquit its functions under the Privacy Act including in relation to providing guidance on data breaches. The ability of the Information Commissioner under section 33C of the Privacy Act to undertake assessments of APP entities relating to the APPs may see data breaches coming to light in addition to those breaches subject to voluntary notification. Furthermore, information about breaches is now regularly revealed when hackers publicly report on their efforts.

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 not to be informed in the event that their personal information becomes compromised, thereby raising the risk they could suffer serious harm. As noted above, more undisclosed breaches may begin to come to light because of the Information Commissioner's powers, and the trend in hackers revealing their work. As also noted above, the OAIC's 2013 national privacy survey found that the large majority of Australians expected entities to be transparent about information security practices, and wished to be informed following loss of their personal information[39]. These kinds of customer preferences may encourage more entities to err on the side of reporting where there has been a breach.

There will be no additional impact on businesses subject to the Privacy Act and they will continue to be able to notify the OAIC of data breaches if they choose to do so. There will be no impact on small businesses as they are generally not subject to the Privacy Act. Larger not-for-profit organisations subject to the Privacy Act (because they have a turnover of greater than $3 million) will be in the same position as organisations that are subject.

[39] Community Attitudes Report, page 5.

Option Two - Introduce a mandatory notification of serious data breach scheme

Who would be affected?

Businesses

Businesses regulated by the Privacy Act would be required to notify the OAIC and affected individuals when personal information has been the subject of a data breach that gives rise to a real risk of serious harm, unless an exception applies. Small businesses which are not subject to the Privacy Act will not be affected.

Individuals

Individuals would be affected by Option Two as they would be notified by entities when their personal information has been the subject of a data breach that gives rise to a real risk of serious harm.

Government

Government agencies regulated by the Privacy Act will be required to notify the regulator and affected individuals when personal information has been the subject of a data breach that gives rise to a real risk of serious harm unless the agency is subject to an exception. Exceptions would apply if notification would impact upon a law enforcement investigation or the operation of a secrecy provision in other legislation, if a data breach fell under existing notification requirements in the MHR Act, or if notification was determined by the regulator to be contrary to the public interest.

The introduction of the option will also affect the OAIC, as it will regulate Option Two.

Benefits

Individuals

Option Two would ensure that individuals at real risk of serious harm due to a data breach are notified of the incident, and receive recommendations about steps they should take in response. The individuals would then 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'. For example, this might allow an individual to change 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.

This is expected to raise confidence amongst consumers about the entities that they are dealing with, and the increased transparency will provide consumers with more information to make informed choices about whether to transact with particular entities.

Businesses

Option Two would require mandatory notification following a data breach of personal information, credit reporting information, credit eligibility information or tax file number information — all of which are subject to existing security requirements in the Privacy Act — that creates a real risk of serious harm to affected individuals.

Requiring notification may act as an incentive to the holders of the above 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 objective, although it has been part of the rationale for data breach notification laws in many other jurisdictions.

The creation of mandatory laws would also create a more level playing field for organisations. The Victorian Privacy Commissioner noted in its submission to 2012 Discussion Paper 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.

Costs

Businesses

The introduction of a mandatory scheme for entities regulated by the Privacy Act raises the question of what new compliance costs will be necessary. It is expected that the overall impact of the option would be low for the following reasons:

- research indicates notification costs amount to only 2.5% of the overall cost of a data breach[40];
- the Privacy Act has a small business exception that would exclude around 94% of Australian enterprises from the proposed scheme[41];
- the OAIC expects only 200 notifications in the first year of the proposed scheme's operation;
- 40% of voluntary notifications the OAIC currently receives are from government agencies and have no cost to businesses;
- the proposed scheme's relatively high notification threshold, and provisions to allow entities to self-assess whether notification is required, will mean fewer notifications are required than comparable schemes in other overseas jurisdictions;
- a simple, streamlined scheme is proposed with the intention that entities who already participate in the OAIC's voluntary scheme will experience minimal change; and
- the OAIC's anecdotal experience is that a large proportion of data breaches occur due to non-compliance with existing Privacy Act security requirements (which is supported by analysis of Privacy Commissioner determinations involving data breaches between 2011 and 2015, which demonstrate a non-compliance rate of 88%); such breaches are, therefore, not a regulatory burden.

Administrative costs

1. 2013 targeted consultation

In the 2013 targeted consultation process, submissions were sought on the proposed mandatory notification model that was introduced to Parliament as the Privacy Alerts Bill. Respondents from a number of industry groups commented that there would be 'paper burden' or administrative costs in complying with the mandatory scheme proposed at that time. In summary, these were described as:

- costs linked to notification methods (e.g. 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

[40] Ponemon Report, page 2.
[41] Based on statistics AGD commissioned from the Australian Bureau of Statistics in 2013.

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 (e.g. 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 2013 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'.

Whilst the views above may be salient for companies without a data breach policy, it is relevant to note that many companies already participate in the voluntary scheme and/or have a relevant policy. A recent report assessed over 100 leading Australian consumer brands against privacy best practices and found over two thirds have a data breach policy[42].

In the 2013 targeted consultation 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.

The timing of the 2013 consultation process may also mean there is a degree of uncertainty about the general cost estimates received from industry. The consultation occurred at a time when entities would have been preparing for the March 2014 commencement of major amendments to the Privacy Act, including new information security requirements in APP 11 and other provisions. Consequently, entities would not have had practical experience applying the post-March 2014 Privacy Act security requirements on which the proposed Privacy Alerts Bill was based, meaning general cost estimates from that consultation process might not be reliable at this stage. It is also unclear whether some cost estimates conflated data breach notification costs with the costs of complying with APP 11 and other new or amended Privacy Act information security requirements (which, as they have been in force since March 2014, cannot be considered part of the regulatory costs arising from Option Two).

The Privacy Alerts Bill was the starting point for Option Two, with changes made to remove unnecessary detail and procedural requirements, provide greater clarity about key terms, and revise the notification processes to introduce more flexibility and reduce costs for entities. Furthermore, the proposed scheme will be largely based on the current voluntary scheme, meaning the cost of the proposed scheme will be minimal on entities participating in the current voluntary scheme.

Further consultation will be undertaken to seek to quantify any costs of the option on businesses.

[42] Deloitte report, page 8.

2. Cost of notification of a data breach

Notification costs will have two components: the costs of notifying the OAIC and the cost of notifying individuals. Notification to the OAIC and affected individuals is only required following a 'serious data breach'. It is expected that the OAIC will issue guidance material that will help entities assess what constitutes a 'serious data breach', and how to comply with the proposed scheme's notification requirements.

Given the magnitude of some data breaches, particularly in an online environment, it is expected that the main costs of notification of a data breach will be the cost of notifying affected individuals. However, the increasing ubiquity of electronic communication using email, social media and web publishing will decrease notification costs when compared to the more traditional forms of communication such as mail and telephone. Whilst a small and decreasing percentage of notification may continue to be by mail and telephone, it is expected that the vast majority of notifications would occur electronically.

Also relevant to the cost of notification is that the option would include mechanisms to ensure that direct notification to affected individuals would not be required if it was unreasonable (for example, if the associated cost to the business would be excessive in all the circumstances). In these circumstances, the business would be able to notify the serious data breach via its website (if any) and any other reasonable methods (such as posts on the business's social media channels, if any, or a newspaper advertisement if appropriate). Particularly in the expected small percentage of situations where a business could only notify affected individuals directly via mail and telephone, these mechanisms would be expected to reduce the cost of compliance for business and prevent businesses from incurring unreasonable notification costs.

Research indicates notification costs amount to a small percentage of the overall cost of a data breach. A 2015 report stated that the average total cost of data breach for an entity was $2.82 million. In contrast, the cost of notifying regulators and affected individuals of a data breach was $0.07 million or 2.5% of the total cost.[43]

The projected amount of notifications under the option is relatively low. Based on the current voluntary scheme and statistics from other jurisdictions, in the first year of the proposed scheme's operation the OAIC expects to receive only 200 data breach notifications.

When assessing the impact of the proposed scheme on businesses it is relevant to note that around 40% of notifications under the current voluntary notification scheme are related to government agencies and have no impact on businesses. Furthermore, one in five notifications under the current voluntary scheme have involved only a single individual's personal information and roughly half of all notifications have involved less than 100 people.

The proposed scheme would only require notification when there is a 'real risk of serious harm' to affected individuals. This threshold is based on the relevant recommendation of the ALRC report and is the same threshold is used in the OAIC's current voluntary scheme. This means that notification would not be required following a data breach where the risk of harm is remote, or the potential harm not serious. This will mean

[43] Ponemon Report, pages 1-2.

notification would be required less often compared to jurisdictions such as California and the European Union, and the impact on businesses would be decreased accordingly.

APP 11 requires regulated entities to take reasonable steps to protect information from misuse, interference and loss and unauthorised access, modification or disclosure. APP 6 requires that personal information should not be disclosed other than for the purpose of collection. Whilst not collecting specific data, the anecdotal experience of the OAIC is that a large proportion of notifications under the current voluntary scheme are a result of failure to comply with the Privacy Act. This is supported by the high percentage of Privacy Commissioner investigations into data breaches that were the result of a breach of the Privacy Act. Between 2011 and 2015 the Privacy Commissioner published 16 investigation reports into data breaches. Of the 16 investigations carried out 14, or 88%, were found to include breaches of the Privacy Act.

The high percentage of data breaches due to Privacy Act non-compliance is likely to be equally high under the proposed option. Therefore, a large proportion of the costs of reporting a breach will come from non-compliance with the Privacy Act, rather than being a cost of complying with the mandatory notification scheme. Also relevant is a finding from the Ponemon Report that where an organisation has strong security measures in place before a data breach, as would be the case for entities who comply with the Privacy Act security requirements, the average total cost of the breach was reduced by as much as $14.50 per compromised record of personal information[44].

3. Cost to small businesses

The proposed scheme will only apply to around 6% of Australian businesses. The Privacy Act exempts small businesses (entities with an annual turnover of $3 million or less) from the operation of the Privacy Act. This exemption does not apply to some businesses, including those that provide a health service, are a credit reporting body, or trade in personal information. The Attorney-General's Department commissioned statistical analysis from the Australian Bureau of Statistics that showed that in 2013 about 94% of entities on the ABS Business Register are below the $3 million threshold and are therefore not likely to be subject to the Privacy Act or the proposed scheme.

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 subsection 6D(4), e.g. they trade in personal information. In the 2013 targeted consultation process, it was argued that mandatory data breach notification would place a disproportionate cost on small businesses which are subject to the Privacy Act, particularly in the direct marketing industry, as they may not be in a position (unlike larger organisations) to absorb some of the costs internally.

4. Cost to not-for-profit organisations

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

5. Cost to particular industry groups

[44] Ponemon Report, page 8.

Respondents to the 2013 targeted consultation process had mixed views about whether particular industry sectors would incur disproportionate costs 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 and start-ups (see Item 3 above); and
- some members of the financial services sector, given that the coverage includes APP regulated entities, credit providers and tax file number recipients.

6. Competition costs

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. In the 2013 targeted consultation stakeholders suggested that, in the US, bigger companies support data breach laws because smaller competitors cannot meet the compliance requirements and some cease doing business. The proposed amendments are unlikely to raise these issues as they do not change the small businesses exemption in the Privacy Act. In addition, individuals who are likely to prefer larger firms due to regulated privacy protections may have already made this choice due to the fact that the Privacy Act already applies to those firms.

Industry group respondents 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. This is supported by the Ponemon finding that, following a data breach, 56% of the costs associated with a data breach were incurred through indirect costs including increased customer 'churn rate' (the percentage of customers abandoning a business)[45]. Ponemon also found (while acknowledging the small sample size) that post-data breach churn rate varied between industries, with the service and financial service industries experiencing a relatively higher churn rate and, as a result, also reporting a higher per capita cost per breach[46].

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, the group's view was that 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 (e.g. 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.

[45] Ponemon Report, pages 1-2.
[46] Ponemon Report, page 9.

Option Two responds to this concern by regulating that the Commissioner, whilst being able to direct the information provided to individuals by entities, would not be able to direct entities on the form of notification. Instead, an entity would have discretion to undertake 'general publication' where notifying each affected individual of a serious data breach would be impracticable, in which case the entity would be required to notify the breach via its website (if any), and to take 'reasonable steps' to publicise the notification. This could include publicising the notification via a newspaper or online advertisement, a social media posting, or any other method that is reasonable in the context of the entity's operations and the circumstances of the data breach.

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, if subject to the Privacy Act, would need to factor in the costs associated with a mandatory data breach notification scheme. However, it is arguable that these costs 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.

Individuals

There is the possibility that as a result of the introduction of a mandatory scheme some entities that need to make internal changes to improve compliance with the Privacy Act and these costs may be passed on to consumers, thereby making transactions more costly.

Government

The impact on the OAIC is likely to be significant. As the regulator, the OAIC 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. The OAIC also expects to receive a higher number of privacy complaints due to complaints from individuals who receive data breach notifications, and that it will also be necessary to use other regulatory powers in some cases (for example, to investigate serious data breach notifications that suggest an entity has systemic privacy compliance issues). The OAIC will be expected to issue new guidance on the new provisions and will 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.

Cost of Option Two

Table 1 calculates the cost to business entities subject to the Privacy Act of the introduction of a mandatory notification serious data breach scheme per annum. The figure is drawn from the OAIC's estimate of the amount of notifications that would occur under the option multiplied by the cost of notifying regulators and affected individuals as reported in the Ponemon Institute's 2015 *Cost of Data Breach Study: Australia* less factors not included in the Regulatory Measurement Burden Framework being:

- agency costs;
- estimated non-compliance costs; and

- estimated costs of relevant notifications (those that would satisfy the threshold for the proposed scheme) under the current voluntary scheme.

Costings for the proposed scheme have been limited to notification costs as:

- the Ponemon Report amount is inclusive of costs for the 'determination of all regulatory requirements',
- 2013 targeted consultation undertaken during the 2013 RIS process was unable to quantify administrative costs to entities, and
- other substantive and administrative costs associated with the proposed scheme would be absorbed into the costs entities incur for general Privacy Act

Table 1: Regulatory burden and cost offset estimate table for Option Two

Average annual regulatory costs (from business as usual)				
Change in costs ($ million)	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$0.8	$0	$0	$0.8
Cost offset ($ million)	Business	Community organisations	Individuals	Total, by source
Agency	$0.8	$0	$0	$0.8
Are all new costs offset? **Yes**				
Total (Change in costs – Cost offset) ($ million) = $0				

Key cost assumptions:

The OAIC projects that if Option Two is implemented the scheme will receive 200 notifications in its first year of operation. This information is based on the OAIC's experience handling voluntary data breach notifications over the past five years, and comparisons with similar overseas jurisdictions.

The Ponemon Report found that, on average, data breach notifications cost $0.07 million per data breach. The report was drawn from an analysis of 23 data breaches in Australia in 2015 with the average number of records breached being 19,788 records. The study describes notification costs to 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. The costing assumes that this is the average of an entity's costs under Option Two.

The OAIC estimates that 41% of notifications are made by Government agencies under the current voluntary data breach notification scheme. The costing assumes the figure would be similar to the proportion of notifications made by Government agencies under this option.

The costing assumes that a large proportion (88%) of data breaches under Option Two would be the result of non-compliance with the Privacy Act and the costs of these notifications are not included in the measurement of the regulatory burden of the option. The Office of Deregulation's (Revised) Guidance Note – *Regulatory Impacts from Non-Compliance and from the Administration of Courts and Tribunals* states non-compliance costs are excluded from the Regulatory Burden Measurement framework and are not required to be considered in a regulatory costing.

As outlined above, the OAIC has indicated that in their experience a large proportion of data breaches involving personal information result from regulated entities failing to comply with APP 11 and APP 6. An assessment of Privacy Commissioner 'Commissioner initiated investigations' suggests 88% of data breaches occur due to non-compliance with the Privacy Act. This costing assumes the rate of non-compliance under Option Two would equal the percentage of non-compliance in Commissioner initiated investigations and excludes them from the costing.

The OAIC has indicated that approximately 40% of the notifications made under the voluntary scheme would satisfy the threshold of Option Two. As the OAIC expects a mandatory scheme will see data breaches notifications double, the costing assumes this would mean 20% of Option Two notifications would also have been made under the voluntary scheme and excludes them from the costing.

Option Two will have an impact on community organisations with an annual turnover of $3 million or more. In Table 1 this impact is captured in the total costs to businesses.

Net benefit analysis

Option Two would provide individuals with notification if breach of their personal information occurs. Concerns about the safety and security of personal information in the online environment have been identified as key issues for individuals (as evidenced in the findings of the OAIC's 2013 national privacy survey cited above). Notification would place individuals in a better 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 and identity theft, which is consistent with US studies mentioned above which indicate mandatory data breach notification laws are effective in lowering identity theft rates.

Option Two is likely to improve business compliance with responsibilities under the APPs. Specifically, Option Two will likely see entities improving their information security practices in line with APP 11 and the requirement to protect the personal information the entity holds from misuse, interference and loss and from unauthorised access, modification and disclosure. Ponemon's analysis suggests that, in turn, better information security practices would help reduce the cost of data breaches (with encryption alone resulting in an average cost decrease of $14.50 or 21% per breached record of information)[47].

A mandatory notification scheme may also make entities focus on how long personal information needs to be retained. APP 11 requires organisations to destroy or permanently de-identify information that is no longer needed for the permitted purposes for which it may be used or disclosed. Improved compliance with this requirement may help avoid data breaches involving information that an entity no longer has any lawful purpose to retain: for example, of the Privacy Commissioner's 16 investigation reports about data breach

[47] Ponemon Report, page 8.

incidents between 2011 and 2015, four involved failure to comply with the Privacy Act's destruction/de-identification requirements (as they applied under the now-repealed National Privacy Principle 4 rather than the current APP 11).

A mandatory notification scheme may also result in improved compliance with rules relating to the collection of personal information. First, an entity is likely to more carefully consider what personal information is it necessary to collect. APP 3 requires private organisations to only collect personal information that is reasonably necessary for one or more of their functions or activities. As noted in the OAIC Data Breach Guide, personal information that is never collected, cannot be mishandled[48].

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 (e.g. 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. Recent research indicates that the notification costs of data breaches is reducing (noting that notification costs are only one component of the costs entities will incur after experiencing a data breach, and that entities will incur other these costs following a data breach regardless of whether notification is mandatory or not)[49].

Whilst the introduction of a mandatory data breach notification scheme may see businesses improving compliance with their obligations under the APPs, the cost of these improvements is not a burden being imposed by the scheme. Rather, any such costs are linked to compliance with extant obligations under the APPs and the Privacy Act that pre-date the introduction of the scheme.

The growth of specific 'cyber insurance' products could also mean that the cost of data breach notifications will not be a burden borne directly by an increasing number of businesses with cyber security coverage. As the frequency and magnitude of data breaches increase insurers' underwriting responses are adapting[50]. Cyber insurance exclusions are being added to general policies, protection is being provided in specific cyber security policies and the purchase of these policies, which can include coverage of the cost of privacy notifications, is increasing[51]. A 2015 global survey with more than 10,000 participants found 59% of respondents had purchased cybersecurity insurance. The survey projected that the cyber insurance market will increase from $2.5 billion this year to $7.5 billion in 2020[52].

---

[48] Data Breach Guide, page 8.
[49] Ponemon Report, page 11.
[50] *Insurance Banana Skins 2015: The CFSI Survey of the Risks Facing Insurers*, pages 16-17.
[51] Eric Lowenstein and Kevin Kalinich, *Recent Australia Privacy Incidents Compared to Rest of World: Insurance Response*, Privacy Law Bulletin April 2015. *Cyber Insurance Research Paper*, Centre for Internet Safety, 2013, pages 7-8.
[52] *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016*, PwC, pages 15-16.

As noted above, 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 (e.g. 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-driven marketing campaigns launched on behalf of other businesses.

Option Three — Encourage industry to develop industry codes

Who would be affected?

Private sector organisations and agencies 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 would be developed under Part IIIB of the Privacy Act, which allows for the Information 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.

Part IIIB codes do not replace or override existing requirements in the APPs. Instead, a code clarifies how particular APPs are to be applied or complied with in a specific industry context. A code may also include obligations that go beyond the requirements of the APPs or the Privacy Act, such as a commitment to undertake data breach notification in specific circumstances.

Benefits

Business

There could be a number of benefits to a particular industry sector in developing an industry code. Firstly, an industry code could give entities a sense of active ownership of their privacy obligations. Secondly, a code 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.

Individuals

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

Costs

Businesses

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 Part IIIB of the Privacy Act, the OAIC Code Guidelines 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;
- scoping and drafting the code;
- seeking legal or professional advice;
- involving all stakeholders (including consumers) in an effective public consultation on the draft code;
- establishing and financing a code administrator to oversee the operation of the code, including reporting on the operation of the code and initiating regular reviews of the code; and
- maintaining information about the code on a website, including a list of the entities bound by the code, where relevant[53].

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 2013 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 code-based mandatory data breach notification is necessary to ensure specialised treatment for a particular industry sector or sectors.

The Privacy Act regulates a wide variety of industries. The Australian and New Zealand Standard Industrial Classification (**ANZSIC**) contains 19 broad industry divisions. There are entities regulated by the Privacy Act in all 19 divisions with numbers ranging from a few hundred to over 10,000 depending on the category. Therefore, any attempt to provide code coverage similar to Option 2 would require multiple codes across multiple industry sectors at what would appear to be a significant duplication of resources.

OAIC

The impact on the OAIC is likely to be moderate to high, depending on its level of involvement in developing and approving each code. As the regulator, it will be expected to promote greater awareness of the OAIC Data Breach 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 and information security

[53] Code Guidelines, pages 4–5.

practices, there may be a longer term decline in the number of data breaches entities experience, which would result in fewer notifications reported to the OAIC and affected individuals.

Cost for Option Three

Table 2 calculates the cost to business entities of the creation of industry specific codes for data breach notifications and the cost of subsequent notifications. The costing includes the estimated cost of code development and the cost of notification under the codes.

Table 2: Regulatory burden and cost offset estimate table for Option Three

Average annual regulatory costs (from business as usual)				
Change in costs ($ million)	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$2.7	$0	$0	$2.7
Cost offset ($ million)	Business	Community organisations	Individuals	Total, by source
Agency	$2.7	$0	$0	$2.7
Are all new costs offset? **Yes**				
Total (Change in costs – Cost offset) ($ million) = $0				

Key cost assumptions

Based on stakeholder consultation, the costing assumes the cost of developing and administering an industry code to be $1 million.

The costing assumes the creation of 19 codes to cover-off all of the industry sectors in ANZSIC.

The costing assumes the cost of notification to businesses would be the same as those under Option Two.

Option Three will have an impact on community organisations with an annual turnover of $3 million or more. In Table 2 this impact is captured in the total costs to businesses.

Net benefit

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 Data Breach Guide, otherwise it is unlikely to receive the Information 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 Two 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. It is also unclear whether it would be feasible to develop industry codes which cover a significant proportion of the entities in each of the 19 individual ANZSIC sectors. In any case, 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 (e.g. telecommunications providers) and may be required to implement different responses to data breaches that occur depending on which code is applicable.

The benefits of Option Three for individual Australians are uncertain, given the difficultly in predicting the number of codes likely to be developed, the quality of those codes, and the number of entities in each industry sector likely to be covered by those codes. Individuals' data breach notification experiences would most likely vary depending on the particular industry that experiences the breach and the nature and coverage of any data breach notification code applying to that industry. Although the OAIC's regulatory oversight and advisory role in a code-based approach might generate consumer confidence (to the extent consumers are aware of that role), unless codes are uniformly adopted across a range of industry sectors, there remains a significant risk that individuals may continue to be kept unaware in the event that their personal information becomes compromised.

It would also be possible for industry to develop data breach notification codes outside of the process in Part IIIB of the Privacy Act. Such codes would have no bearing on entities' obligations under the Privacy Act, and the OAIC would have no direct regulatory oversight and advisory role over such codes. 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 Data Breach Guide and recommended by the ALRC. The different requirements that would apply across industry sectors would also be 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

Previous consultation

A mandatory data breach notification scheme has been the subject of extensive consultation to date:

1. the ALRC report was the subject of consultation before it was released in 2008;

2. in 2012 the Attorney-General's Department received submissions to the 2012 Discussion Paper on the introduction of a scheme;
3. in 2013 targeted consultation was undertaken with stakeholders seeking comments on a legislative proposal that would become the Privacy Alerts Bill, which is the basis of the current Option Two; and
4. in 2013 the Legal and Constitutional Affairs Legislation Committee sought and received submissions on the Privacy Alerts Bill.

Have your say

The Government invites stakeholders to comment on this Consultation Draft Regulatory Impact Statement (**Consultation Draft**). Submissions are invited by 4 March 2016.

In addition to seeking general submissions on the Consultation Draft, we are also seeking specific information in an attempt to quantify the regulatory burden of a mandatory data breach notification scheme. To this end, stakeholders are invited to respond to 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 Serious Data Breaches Bill?
   In particular, what will be the burden to ensure compliance with the mandatory scheme for entities that:
   i. have existing systems in place to make notifications (where necessary) consistent with the existing voluntary OAIC Data Breach Guide; and
   ii. have no existing data breach notification systems in place?
   What will be the ongoing compliance burden?
2. What form of communication would organisations foresee utilising to notify affected individuals of a serious data breach?
3. How can a mandatory data breach notification scheme be implemented in a cost effective manner?

The preferred method of receiving submissions is via email to privacy.consultation@ag.gov.au, using the Submission to the Serious Data Breach Notification Consultation template below.

Written submissions can also be sent to:

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions on its website that have been submitted electronically.

If submitters choose to provide a separate document instead of using the submission template, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)

- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be published on the Attorney-General's website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	
Contact details *(one or all of the following: postal address, email address or phone number)*	

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- ☐ Microsoft Word
- ☐ Rich Text Format (RTF)
- ☐ txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? YES / NO

Your submission

Insert your text here and send the completed submission to the Attorney-General's Department, preferably via privacy.consultation@ag.gov.au