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

Via email to: privacy.consultation@ag.gov.au

7 March 2016

Re: Serious Data Breach Notification Consultation - CLPC submission

Dear Sir/Madam,

Cyberspace Law and Policy Community at UNSW Faculty of Law (CLPC) appreciates the opportunity to provide this submission in relation to this consultation. See attached document.

Regards,

Dr. Alana Maurushat
[contact details redacted]

Mr. David Vaile
[contact details redacted]

CYBERSPACE LAW & POLICY COMMUNITY

Serious Data Breach Notification Consultation

Submission to Attorney-General's Department

Melinda Bolton, Lauren Stubbs, Alana Maurushat, David Vaile, and Kendy Ding

---

7 March 2015

1. Executive Summary

1.1. The Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Privacy Amendment Bill) is a step forward in terms of the protection of personal information, and requiring those holding this information to notify relevant parties when its security is breached – ideally enabling the data subjects affected to take appropriate remedial action, if this is possible, in a timely fashion. Unfortunately, the obligations of those required to notify individuals of data breaches are not made clear in the exposure draft of the Bill, and there are other flaws.

1.2. This submission includes information about our research on mandatory data breach notification laws in other jurisdictions, particularly the many states in the US with such laws (see Appendix 1 for a summary of the incidence of key features of these laws). Researchers at CPLC have been tracking data breach notification laws and incidences globally since 2007. The Australian Privacy Amendment Bill has borrowed a number of ideas from the United States, and in some aspects has improved upon problematic aspects of their approach. For example, the Bill describes the content that should be included in the notification, introduces a harm threshold in an attempt to reduce excessive or trivial notification and 'notification fatigue,' and incorporates good practice guidelines in Australian Privacy Principle 11.1.

1.3. We support the introduction of mandatory Data Breach Notification legislation. It is better than not having any such law in Australia. However, this Bill presents has some shortcomings which should be addressed before it is introduced, including the following:

1.3.1. it does not make it clear what an entity's obligations are. These should be spelled out clearly and explicitly.

1.3.2. the harm threshold is largely self-determined by the Australian entity (an assessment made more difficult by vague legislative provisions). There should be more guidance on this threshold, and objective indicators should be included. The threshold should not be set artificially high.

1.3.3. there is a seemingly full-proof encryption exemption

1.3.4. there is no duty to report breaches to credit reporting agencies when encryption is used. As such Australia will continue to have poor metrics for measuring breach

incidences. This leads to difficulties for cyber-insurance, and for formulating better policies around data breach.

1.3.5. there is no private right of action or class action.

2. Recommendations

1. Provide examples, in the legislation, of types of data that will be considered 'personal information' for the purposes of the new provisions. This list does not need to be conclusive or exhaustive, but it should give clear guidance to entities seeking uphold their obligations under the Act. This should include reference to information that is included by virtue of the operation of other legislation, such as that recently enacted for the new data retention scheme.

2. The limited circumstances under which alternative notification arrangements may be warranted and permitted should be more clearly set out. These alternatives should encourage the use of the most efficient methods of effective direct notification, rather than indirect mass media publication as 'substitute service'. Given the data custodian will generally have effective contact information for each affected data subject, and will data processing capability proportional to the size of the data set, modern communication and messaging tools can have very low marginal cost, so traditional concerns about expense and practicality have limited justification if cost effective direct methods are accepted. Any notification alternatives which do not involve direct notification should be a last resort, and require authorisation by the commissioner.

3. A provision should be added to compel entities to notify relevant consumer reporting agencies of any breach deemed serious enough to require notification. Alternatively, the provision could compel entities to notify relevant consumer reporting agencies of breaches that reach a certain threshold (i.e. 1,000 affected individuals). (This may or may not require amendment to existing provisions such as the credit reporting scheme in the *Privacy Act.)*

4. Set out specific penalties for entities in contravention of the legislation. For example, a specific monetary penalty per breach, and an ongoing daily penalty for continued non-compliance. The *Spam Act 2003* (Cth) offers an effective model.

5. Section 26WB(3) should be amended in order to make an entity's role clearer. It should state that it is the entity who bears the onus of making the decision, that they 'may' have regard to the factors listed in ss(a)-(j), and subsection (e) should be deleted. If ss(a)-(j) are kept, it should be clear that they are non-exhaustive suggestions and the entity's responsibility should be to conduct a prompt and robust investigation into whether there is a real risk of harm serious enough that some or all data subjects would have reasons for needing to be notified (such as to be able to assess implications of the breach for their particular circumstances, and their need to consider individual action to mitigate, stop or investigate any loss).

6. Further, while only breaches reaching the harm threshold needs to be reported to individuals, all breaches should be reported to the Privacy Commissioner, and basic details of the breach should entered by the custodian onto a breach notification register accessible online. This adds a safeguard and transparency to the process, and gives more practical effect to s26WD, while requiring very limited effort for breaches with limited impact, and no 'noise' of excessive notifications for data subjects when the breach is trivial rather than serious.

7. Notification should be also compulsory upon the breach of encrypted data. Encryption cannot be assumed to be so completely effective in securing personal information subject to a breach, or to so completely prevent all breach-related harms, as to justify removing the normal expectation that the data subject should be notified. If encryption is to have an incentive in this legislation, it should be in the form of its recognition as good practice when the question of remedies and reasonable precautions arise, not as a means to negate the right and expectation that a data subject is informed of a serious breach.

8. A variation on this is for Section 26WB(3)(d) to be altered to make clear that if data is likely to be decrypted, the encryption key is likely to be accessed or misused, or the encryption is otherwise likely to be ineffective to protect the data, these are relevant matters for consideration when assessing whether the breach creates a real risk of serious harm. However, ascertaining the actual level of this risk is likely to be increasingly difficult as diverse means of compromising the protective effect of encryption are constantly enhanced (whether at the sophisticated end by quantum computing advances in brute force, or at the crude end by social engineering, coercion, hacking, introduction of malware or compromised operating systems, exploitation of bugs, or operational mistakes). So where there is doubt or uncertainty about the current level of actual vulnerability of a particular data set under encryption, a precautionary approach assuming a significant risk is reasonable and should be required. Eg, if in doubt, assume the encryption may not offer perfect protection, and notify.

9. A provision should be added to outline the obligations of third parties when notification is required. Third parties should be able to conduct their own investigation but the approval, and/or inclusion, of the data owner should be required, and the owner should be the entity to notify individuals, as is done in the US.

10. Industry standards that focus directly on the prevention of data breaches (i.e. mandatory encryption of data, minimisation of unnecessary collection and distribution, avoidance of centralised 'honey-pots', privacy impact assessment, regular unannounced external information security and intrusion auditing, security and breach prevention training and evaluation programs, treating personal information security on a par with financial information security for auditing and governance purposes, board or C-level responsibility for data breach prevention and response, etc.) should be promoted and, where externally verified as effective, recognised as good practice.

3. Introduction

4.1 Data breach notification and disclosure laws are emerging around the globe. In essence, data breach notification legally requires corporations and organisations to notify individuals when a breach of security leads to the disclosure of personal information. This is promulgated under the theory that consumers have a right to know when their personal information has been stolen or compromised. It is believed that this knowledge will encourage individuals to take action to minimise the adverse effects of a breach. Equally so, it is hoped that data breach notification legislation will provide an incentive for corporations and organisations to take adequate steps to secure the personal information that they hold.

4.2 The scope of notification laws varies greatly from country to country. Many countries such as the United States, The European Union and Australia have tabled Bills or passed legislation that provides for mandatory data breach notification. Other jurisdictions such as Canada and Japan have instituted voluntary guidelines. In many jurisdictions, data notification is sector specific (e.g. banking and financial sector or the telecommunications sector). Many of the current

proposals, guidelines and laws (Australia included) borrow from the experience of the US, which is outlined in Appendix One. The below is an evaluation of the draft Privacy Amendment Bill in comparison with the US framework. A particular focus is placed on the ability of entities to gauge what their obligations to consumers are in the event of a breach of personal information.

4. Personal information

4.1 The definition of personal information is found in the General Definitions section of the *Privacy Act* 1988 (Cth). It is defined as "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."[1] This definition is broad, citing no specific types of information that might be considered to be personal information.

4.2 This differs greatly from the US jurisdictions whereby each state specifies a driver's license number, social security number and financial account numbers in conjunction with the first name or initial and last name of the individual at a minimum. Further, states such as Iowa and Oregon include data such as biometric information and medical information under their definition of personal information.

4.3 It is somewhat beneficial to have a definition that is broad enough to entail numerous types of information that do not limit the need to notify. However, providing a specific definition for what constitutes personal information means that entities do not have to perform a lengthy investigation to determine whether the information subject to the breach is in fact personal information. Rather they need only look at whether or not the breach of such data presents a real risk of serious harm to the individual. This is beneficial in that it expedites the process of investigation and makes it less complicated for the entities on which the burden to investigate falls.

Recommendation 1: Provide examples in the legislation of types of data that might be considered personal information. This list does not need to be conclusive, but should give clear guidance to entities seeking uphold their obligations under the Act.

This should include reference to information that is included as 'personal information' by virtue of the operation of other legislation, such as that recently enacted for the new data retention scheme.

5. Form and content of notification

5.1. Method of communication

5.1.1. Following a recommendation by the ALRC that correspondence stand alone and not be bundled with other correspondence the Privacy Amendment Bill states that the method of communication should be determined by the agency's or organisation's ordinary methods of communicating with the individual.[2]

5.1.2. The method of notification used in US jurisdictions is a prominent aspect of

[1] *Privacy Act 1988*, Part II Interpretations Division 1 General Definitions.
[2] Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, s26WC(4).

their legislation. Each state sets out guidelines on how individuals should be contacted. At a minimum it specifies that individuals can be notified by written notice, telephone or through electronic mail if this is the way that the organisation normally communicates with the individual. This is similar in effect to the Australian Bill. Other states, such as Hawaii go into more detail, identifying specific ways in which individuals can be contacted by telephone. For example, those individuals should not be contacted by a pre-recorded phone message (sometimes called a 'robo-call', a technique often also used by offshore telemarketers and scammers and intrinsically difficult to authenticate or trust).

5.1.3. The Privacy Amendment Bill would be improved by guidance about what methods of communication may be considered inappropriate (for instance, a robo-call would generally be deprecated), but making clear that efficient methods such as email, SMS, text or other personally addressed communication in a channel known to be used by the affected person are permissible. This is to both avoid suspicious or disrespectful methods (robo-calls), and to encourage avoidance of costly means where others work acceptably for the purpose of reliable direct notification.

5.2. Substitute notice

5.2. The Privacy Amendment Bill does not provide a specific threshold for substitute notice. Section 26WC merely states that if it is not *practicable* for an entity to notify each individual they must publish a copy of the statement on their website and take reasonable steps to publicise the content of the statement.[3] This has the disadvantage of vagueness, and no guidance as to thresholds for practicability assessment. It has the advantage that the scale of the effort is linked to the scale of the breach, and given that the beneficiary of the provision is the data subject, it means that large breaches will require contacting every individual affected, where the custodian has practicable means for communicating directly, as will often be the case.

5.2.1. Almost all US jurisdictions have a threshold for substitute notice. This means that if notice is likely to exceed a certain amount (e.g. $250,000) or a certain number of individuals (e.g. 2,500), then the entity may use a substitute form of notice. This would include a conspicuous posting to their website and notification to state wide media.

5.2.2. The US legislation often specifies the circumstances that would render it 'impractical' to notify individuals. This is cheaper for the organisation but deprives the individual of what would otherwise be their right to be directly notified if their information has been breached. This means entities have an understanding of when they need to notify individuals individually and directly and when they can notify large classes of affected individuals indirectly by public communications. Without this detail, entities may struggle to understand what is required of them, and also may be tempted to 'cry poor' by use of expensive methods as an excuse to trigger this exemption. However, the cost profile of notification methods for individuals whom the custodian already retains records is potentially very low.

[3] Ibid, s26WC(1)(d).

5.2.3. To avoid the prospects of abuse of this option, any such substitute provision should include the following safeguards:

- set the threshold for this exemption from normal expectations of individual notification very high, indexed, for instance: a cost of $10 million or 1 million affected individuals. Even for very large numbers of affected people, the normal expectation should be that an organisation capable of dealing with the information of a large number of people, and putting the data protection interests of each of them at risk as a result of a breach, is also capable of dealing with what should a relatively low cost effort to notify them individually. (Only in exceptional cases should this exemption be triggered, otherwise it will be open to abuse.)

- require alternative cheaper methods to be explored (such as automated mass email, notification on customer accounts or log in screens etc.) and the exemption only be available where the cheapest practicable option (not the most expensive, or traditional, option) exceeds the threshold

- even where alternative mass notification methods are permitted, require the organisation to use all practicable methods to draw attention to the existence of the notification in other personalised contacts with the individual.

5.2.4. On balance, the creation of a new exemption for substitute service would not be beneficial for data subjects in the Australian Bill. The US experience could be drawn on to identify efficient means of direct communication.

Recommendation 2: The limited circumstances under which alternative notification arrangements may be warranted and permitted should be more clearly set out. These alternatives should encourage the use of the most efficient methods of effective direct notification, rather than indirect mass media publication as 'substitute service'. Given the data custodian will generally have effective contact information for each affected data subject, and will data processing capability proportional to the size of the data set, modern communication and messaging tools can have very low marginal cost, so traditional concerns about expense and practicality have limited justification if cost effective direct methods are accepted. Any notification alternatives which do not involve direct notification should be a last resort, and require authorisation by the commissioner.

5.3. Notification to consumer reporting agencies

5.3.1. The Privacy Amendment Bill does not require entities to notify consumer-reporting agencies upon discovery of a breach. The entity has poor security policies, data is breached, losses and harm to individuals ensues and the organisation must then notify the individual and the Privacy Commissioner.

5.3.2. The burden of data breach is then shifted to the individual. The individual must contact various credit-reporting agencies to rectify the situation, or at least attempt to. Depending on the types of personal data breached, the individual may have to take further steps (e.g. getting a new license or credit card and notifying the appropriate authorities). The organisation, even if millions of dollars were stolen, has no obligation to report to law enforcement, and may not even have to notify at all if they used encryption.

5.3.3. Contrastingly, many US jurisdictions have provisions providing that, where a certain number of individuals need to be notified (eg. 1,000), then all consumer-reporting agencies that compile and maintain files on consumers on a nationwide basis must also be notified. This means that the individuals do not have the burden of notifying the agency themselves.

Recommendation 3: A provision should be added to compel entities to notify relevant consumer reporting agencies of any breach deemed serious enough to require notification of subjects. Alternatively, the provision could compel entities to notify relevant consumer reporting agencies of breaches that reach a certain threshold (i.e. 1,000 affected individuals). (It is unclear whether this would require amendment to existing provisions such as the credit reporting scheme in the *Privacy Act.)*

5.4. Content of notification

5.4.1. Most US jurisdictions do not specify the contents of the notification. However, some states, such as California and Florida specify that the notice should contain the type of personal information that has been breached, the steps taken to ensure no further breach occurs and information on how to prevent a further threat of identity theft. Requiring these details to be included in the notice ensures that individuals are in the best possible position to protect their personal information. The Australian legislation is strong in its position on contents of the notification. Section 26WC(3) provides a comprehensive list of information that is useful to the individual.

6. Penalties

6.1. The Australian legislation differs greatly in relation to penalties from other jurisdictions. Section 13(4) of the Privacy Amendment Bill states that if an entity is found to be in contravention of either ss26WC or 26WD then it will be considered to be an 'interference with the privacy of an individual'. According to the explanatory memorandum, this means that the Privacy Commissioner will have the power to undertake investigations, make determinations, seek enforceable undertakings and pursue civil penalties for serious or repeated interferences with privacy.[4] Therefore, under Part III Division 1of the *Privacy Act*, the Privacy Commissioner holds discretionary powers to decide when serious penalties should apply. However, it is expected that less severe actions, such as apologies or compensation payouts will be preferred. There is no private right of action for individuals under the Australian framework.

6.2. In the US penalties differ from state to state. The majority of states legislate that a failure to notify of a data breach authorises a civil action to be bought by the state Attorney General and in some cases, the individual. There are some states that do specify monetary penalties. It is essential to recognise that the dissemination of data breach notification laws is in part useful to provide incentive for entities to protect data. The ALRC states that including a civil penalty in the legislation would encourage entities to train staff adequately on best practice standards and to use encryption to keep data secure.[5]

6.3. The use of "softer" penalties under the Australian legislation implies that prevention of a data breach is not one of the purposes of the amendment. Whilst it is important that individuals are notified when their data is breached so that they can take appropriate steps to avert further

[4] Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, 9.
[5] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 51.108, http://www.alrc.gov.au/publications/report-108

harm, preventing data breaches is also an important aspect of data breach notification legislation. If entities are aware of what penalties a failure to notify will attract, then they will be more likely to take measures to ensure that breaches do not occur in the first place, or upon a breach will endeavour to notify the affected individuals with the utmost legislative compliance. Research finds that globally, one of the main drivers for entities using encryption is to protect the organisation's brand or reputation if a breach is to occur.[6] This supports the proposition that a civil penalty would encourage entities to comply with legislative provisions which provide encryption safe harbours.

Recommendation 4: Set out specific penalties for entities in contravention of the legislation. For example, a specific monetary penalty per breach, and an ongoing daily penalty for continued non-compliance. The Spam Act 2003 (Cth) offers an effective model.

7. Best Practice Standards

7.1. Data breach notification legislation in the US does not commonly focus on the implementation of best practice standards in relation to protection of personal information. Most states do not have a security requirement. The states that do have a provision requiring the implementation of a best practice standard usually state something along the lines of 'entities will take appropriate measures to ensure the safe keeping of data'.

7.2. Whilst the Privacy Amendment Bill does not have a provision within itself for best practice standards, the *Privacy Act* already requires entities covered under the Act to take such steps as are reasonable to protect the information they hold under Part 4 Principle 11. Compared to the jurisdictions in the US these requirements are more detailed and comprehensive.

8. Determining when there is a 'serious risk of harm'

8.1. Though it is not specifically stated in s26WB, the legislation as a whole implies that it is the entity themselves who decides whether a serious breach has occurred and subsequently whether notification should be made. This means that the entity must take into account all relevant matters listed in s 26WB. The balancing of these matters, many of which are vague and undefined, means that the entity is at greater risk of misinterpreting the legislation. If an entity misinterprets the legislation and does not notify because they believe a serious breach has not occurred, they are then liable to penalties. More importantly, the data subject is deprived of notice and thus the opportunity to respond and mitigate risk as quickly as may be needed.

8.2. For example, subsection (f) states: "whether the information is protected by one or more security measures." Subsection (f) then repeats this adding " – the likelihood that any of those security measures could be overcome." From the perspective of an entity trying to determine their obligations this is confusing. Subsection (e) merely discusses the use of security measures, with no mention of their quality or effectiveness. This is not a high enough standard if we are talking about breaches in which there is a real risk of serious harm to consumers. Subsection (f) however, ensures that the likelihood of a security measures success is considered and as such should be preferred.

[6] Ponemon Institute, 2011 Global Encryption Trends Study available at http://www.ponemon.org/local/upload/file/2011_Global_Encryption_Trends_Study_FINAL.pdf , 8.

8.3. This section does not clearly set out what it is that the entity should consider in making a determination. For example, it does not state whether the entity 'may' or 'must' have regard to ss(a)-(j). This is an important distinction to ensure the legislation does not provide an overly specific unreachable standard. Given that ss(j) states that "any other relevant matters" may be considered, it may be that ss(a)-(j) should be treated and framed as an indicative guide and not a strict list of matters to consider.

8.4. In the US jurisdictions, it is also an internal decision about whether notification should be made. However, most jurisdictions have the requirement that notification is to be made after any breach of data, thus there is no threshold for seriousness. This means that entities are less likely to mistakenly refrain from notifying individuals. In some US states a harm threshold is used for determining an organisation or corporations obligation to notify affected individuals. For example, in Arkansas notification need only be made if after a reasonable investigation the person or business determines that there is a reasonable likelihood of harm to the consumers. They do not however, set out a list of complicated factors for an entity to consider.

Recommendation 5: Section 26WB(3) should be amended in order to make an entity's role clearer. It should state that it is the entity who bears the onus of making the decision, that they 'may' have regard to the factors listed in ss(a)-(j), and subsection (e) should be deleted. If ss(a)-(j) are kept, it should be clear that they are non-exhaustive suggestions and the entity's responsibility should be to conduct a prompt and robust investigation into whether there is a real risk of harm serious enough that data subjects would have reasons for needing to be notified (such as to be able to assess implications of the breach for their particular circumstances, and their need to consider individual action to mitigate, stop or investigate any loss).

Recommendation 6: Further, while only breaches reaching the harm threshold need to be reported to individuals, all breaches should be reported to the Privacy Commissioner, and basic details of the breach should entered by the custodian onto a breach notification register accessible online. This adds a safeguard and transparency to the process, and gives more practical effect to s26WD, while requiring very limited effort for breaches with limited impact, and no 'noise' of excessive notifications for data subjects when the breach is trivial rather than serious.

8.5. Encryption safe harbor

8.5.1. In the US jurisdictions, there exists an encryption safe harbour. It works upon the presumption that if data is encrypted then there is no serious risk of harm if a breach occurs. The Australian legislation mimics this presumption in ss 26WB(3)(c) and (d). It is presumed that the use of the phrase "intelligible to an ordinary person" relates to the use of encryption to protect data. This implies that if the data is encrypted then there is no real risk of harm as it is unlikely that information could be used in identity theft crimes. The underlying assumption in both the US and Australia is that encryption creates safe holds around information to make it completely secure.

8.5.2. However, encryption is not secure as it is possible to decrypt information. The fact that it is difficult to decrypt data should not lead to the presumption that it is not possible in a given situation, or that it is so highly unlikely it can be disregarded.

8.5.3. The language used in s 26WB(3)(c) and (d) is problematic as the phrase "ordinary person" is arbitrary and in appropriate when referring to information stored in computer databases. The use of encryption means that, of course, data will not be intelligible to an ordinary person. But, that does not mean that the data cannot be decrypted and read by a machine, that it cannot be made to be readable again. Neither jurisdiction applies an obligation on entities to notify where an encryption key has been stolen or compromised, or where there is some other compromise of the effectiveness and reliability of an encryption scheme.

8.5.4. The explanatory memorandum states that the phrase "intelligible to an ordinary person" was used so that this provision may remain technology neutral.[7] The rapid evolution of technology means that the legislation surrounding it must be adaptable and able to respond to changing needs. The technology neutral language in this legislation does not lend itself to adequate protection for those whose data is being kept in computer databases. The provision also does not adequately address the growing threats to the protection offered by encryption.

Recommendation 7: Notification should be compulsory upon the breach of encrypted data.

Encryption cannot be assumed to be so completely effective in securing personal information subject to a breach, or to so completely prevent all breach-related harms, as to justify removing the normal expectation that the data subject should be notified. If encryption is to have an incentive in this legislation, it should be in the form of its recognition as good practice when the question of remedies and reasonable precautions arise, not as a means to negate the right and expectation that a data subject is informed of a serious breach.

Recommendation 8: A variation of this would be for Section 26WB(3)(d) to be altered to make clear that if data is likely to be decrypted, the encryption key is likely to be accessed or misused, or the encryption is otherwise likely to be ineffective to protect the data, these are relevant matters for consideration when assessing whether the breach creates a real risk of serious harm.

However, ascertaining the actual level of this risk is likely to be increasingly difficult as diverse means of compromising the protective effect of encryption are constantly enhanced (whether at the sophisticated end by quantum computing advances in brute force, or at the crude end by social engineering, coercion, hacking, introduction of malware or compromised operating systems, exploitation of bugs, or operational mistakes). So where there is doubt or uncertainty about the current level of actual vulnerability of a particular data set under encryption, a precautionary approach assuming a significant risk is reasonable and should be required.

Eg, if in doubt, the custodian should assume the encryption may not offer perfect protection, and thus notify. This is close to the simple requirement in Recommendation 7 above.

[7] Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, 15.

8.6. Notification Fatigue

8.6.1. By applying a threshold of 'serious harm' the risk of notification fatigue is less likely. According to the ALRC report setting the threshold high should reduce notification fatigue, where individuals receive so many notices of data breaches that it becomes difficult to assess which ones carry a real risk of serious harm and which are minor in nature and consequence.[8] The higher threshold will also reduce the compliance burden placed on corporations and organisations.

9. What are the obligations of third parties?

9.1. The Privacy Amendment Bill is silent on the obligations of third parties. Third parties are often data managers as most organisations outsource their data management. Outsourcing may also follow a chain whereby an organisation contracts with a data management company who then subcontracts with a smaller company and so forth.

9.2. An Australian agency or organisation trading personal information would under most circumstances fall within the framework of the Australian Privacy Principles and would as such be subject to the Privacy Amendment Bill. Section 26WB(5) outlines the obligations of overseas entities. It states that if an APP entity has disclosed personal information to an overseas recipient, Australian Privacy Principle 8.1 applied to the disclosure and the overseas recipient holds the personal information then s26WB applies as if the information was held by the APP entity and the entity were required under s15 of the Privacy Act not to engage in an act or practice that breaches Australian Privacy Principle 11.1 in relation to the personal information.

9.3. Whilst it is clear that third parties fall within the legislative framework the Bill does not make it clear upon whom the onus of notification falls. The US frameworks, for example, make a clear distinction between data owners/licensors and data maintainers. In most states data maintainers are to notify the licensors of the breach and the licensors then go about notifying consumers in a manner compliant with the relevant legislation.

9.4. The further difficulty for Australia is that due to the need for an investigation to determine if there is a real risk of serious harm the legislation in this context would also need to specify who is to conduct the investigation and subsequently make a decision regarding notification.

> **Recommendation 9**: A provision should be added to outline the obligations of third parties when notification is required. Third parties should be able to conduct their own investigation but the approval, and/or inclusion, of the data owner should be required, and the owner should be the entity to notify individuals, as is done in the US.

10. Does data notification prevent data breaches?

10.1. A major issue with data breach notification legislation is that it is a reactive scheme rather than preventative. It is assumed that by implementing data

[8] Australian Law Reform Commission, *For Your Information*: *Australian Privacy Law and Practice*, Report No 108 (2008) 51.86, http://www.alrc.gov.au/publications/report-108.

breach notification organisations will take steps to prevent data breaches. However, corporations often only implement protection mechanisms, such as encryption, after a breach has occurred and the harm already suffered.[9]

10.2. In order to counter this problem VISA developed best practice procedures that mandate the encryption of cardholders' data from the moment the card is swiped to its receipt in a database at the backend.[10] This does not mean that the act of encryption should remove an organisation from obligations under the legislation. Rather, standards of this type encourage development of industry norms for how personal information should be stored most safely.

10.3. Not only does data breach legislation not necessarily encourage companies to protect data at a higher standard, in some cases it also does not seem to reduce the instances of breaches (though the latter may be a result of the former). For example, in the Carnegie Mellon Study states with data breach notification were compared with those without. It was found that there was no "statistically significant result" in rates of identity theft and fraud with those states with data breach laws.

10.4. Furthermore, data breach legislation does not fully address the ways in which personal information is stored. Such frameworks often only look to the protection of data kept on the databases of companies and organisations. This fails to take into consideration the vast amount of personal information kept, and subsequently compromised or stolen, from personal computers and devices. This however, is a further concern that may need to be dealt with in a separate framework.

10.5. To address these experiences in some other jurisdictions, attention needs to be paid to how to encourage raising the standard and adoption of practices that can reduce the incidence of data breach. This may require reconsideration of practices which have grown up under the assumption that data breach is rare and can be reliably be prevented, rather than increasingly common and increasingly hard to prevent in effectively. It may also require raising the profile of personal information security auditing and governance level responsibility, to ensure transparency and top level commitment to prevention efforts.

Recommendation 10: Industry standards that focus directly on the prevention of data breaches should be promoted and, where externally verified as effective, recognised as good practice.

[9] Privacy Rights Organisation, "A Chronology of Data Breaches" available at http://www.privacyrights.org/ar/ChronDataBreaches.htm

[10] VISA Card, 'Issuer PIN Security Guidelines', November 2010 available at https://usa.visa.com/dam/VCOM/download/merchants/visa-issuer-pin-security-guideline.pdf; VISA Card, 'Encryption and Tokenization: Protecting Customer Data available at https://usa.visa.com/content/dam/VCOM/download/merchants/encryption-tokenization-09182013-public.pdf.

(Examples include: mandatory encryption of data, minimisation of unnecessary collection and distribution, avoidance of centralised 'honey-pots', privacy impact assessment, regular unannounced external information security and intrusion auditing, security and breach prevention training and evaluation programs, treating personal information security on a par with financial information security for auditing and governance purposes, board or C-level responsibility for data breach prevention and response, etc.)

APPENDIX 1: Data Notification across the United States

Key:

Y = yes

N = No

YL = Yes but limitations apply (i.e. may only be required if a certain number of breaches occur)

Information compiled February 2016	Alaska Statute s45.48.010	Arizona s44-7501	Arkansas Code 1987 4-7-110	California Civil Code SB1386	Colorado Revised Statutes s6-1-716	Connecticut General Statutes s36a-701b	Delaware Code s12B	Florida Statutes s501.171	Georgia Code s10-1-910-915	Hawaii Civil Code 11-4-487N-1	Idaho Statutes 21-51	Illinois Compiled Statutes 815 ILCS 530/5	Indiana Code s24-4.9	Iowa Code 715C	Kansas Statutes 50-7a	Kentucky Revised Statutes 365.732	Louisiana Revised Statutes Title 51	Maine Revised Statutes s1347	Maryland Code 14-35	Massachusetts General Laws s93H-1	Michigan Identity Theft Protection Act	Minnesota Statutes 325E	Mississippi Code s75-24-29	Montana Code 2-6-15	Nevada Revised Statutes s603A	New Hampshire Revised Statutes 359C	New Jersey Statutes s56:8-161	New York Consolidated Laws 899-AA & 209	North Carolina General statutes 75-2A	North Dakota Century Code 51-30	Oregon Revised Statutes 14-646A	Pennsylvania Statute Title 73 Chapter 43	Rhode Island 11-49.3-2	South Carolina Code 30-1-90	Tennessee Code 47-18-21	Texas Code s521.002	Utah Code s13-44	Vermont Statutes 2430	Virginia Code s18.2-186.6	Washington Code 19-255-010	West Virginia Code s46A-2A	Wisconsin Statutes s134.98
Types of data																																								
Actual (A) or proposed (P) or guideline (G)	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Driver's license number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Financial account number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Debit card number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Credit card number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Personal identification number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Electronic identification number			Y	Y										Y											Y															
Employer identification number																					Y								Y	Y									
National ID (i.e. social security)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Routing code																																								
Digital signature																													Y	Y									
Biometric data														Y																	Y				Y					Y
Fingerprints														Y																	Y									
Financial account passwords	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mothers maiden name																					Y								Y	Y									
Address																					Y																		
Date of birth																													Y	Y									

Information compiled February 2016	Alaska Statute s45.48.010	Arizona s44-7501	Arkansas Code 1987 4-7-110	California Civil Code SB1386	Colorado Revised Statutes s6-1-716	Connecticut General Statutes s36a-701b	Delaware Code s12B	Florida Statutes s501.171	Georgia Code s10-1-910-915	Hawaii Civil Code 11-4-487N-1	Idaho Statutes 21-51	Illinois Compiled Statutes 815 ILCS 530/5	Indiana Code s24-4.9	Iowa Code 715C	Kansas Statutes 50-7a	Kentucky Revised Statutes 365.732	Louisiana Revised Statutes Title 51	Maine Revised Statutes s1347	Maryland Code 14-35	Massachusetts General Laws s93H-1	Michigan Identity Theft Protection Act	Minnesota Statutes 325E	Mississippi Code s75-24-29	Montana Code 2-6-15	Nevada Revised Statutes s603A	New Hampshire Revised Statutes 359C	New Jersey Statutes s56:8-161	New York Consolidated Laws 899-AA & 209	North Carolina General statutes 75-2A	North Dakota Century Code 51-30	Oregon Revised Statutes 14-646A	Pennsylvania Statute Title 73 Chapter 43	Rhode Island 11-49.3-2	South Carolina Code 30-1-90	Tennessee Code 47-18-21	Texas Code s521.002	Utah Code s13-44	Vermont Statutes 2430	Virginia Code s18.2-186.6	Washington Code 19-255-010	West Virginia Code s46A-2A	Wisconsin Statutes s134.98
Medical information			Y	Y				Y			Y					Y								Y				Y	Y	Y		Y							
Telecommunications device																																							
Tax file number																Y			Y		Y			Y															
Passport																					Y										Y							
Health insurance information			Y	Y				Y			Y										Y									Y	Y		Y			Y			
Username/email address			Y	Y				Y			Y																					Y						
NAME IN COMBINATION WITH DATA TYPE	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Standards applied																																						
Encrypted data safe harbour	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
'Material risk of risk'																																Y						Y
External determination																																						
'Reasonable likelihood of harm'			Y										Y								Y										Y				Y			
'Any breach' provision	Y	Y		Y		Y		Y	Y	Y		Y	Y			Y	Y			Y		Y	Y		Y		Y	Y	Y	Y		Y	Y		Y	Y		Y	
Misused or likely to be misused					Y		Y				Y				Y			Y	Y							Y								Y				
Cases or is reasonably likely to cause loss or harm																																						
Procedure following breach/leak																																						
Notice to privacy commissioner (or equivalent)								Y										Y								Y												
Data owner/ licenser notify individuals	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Data Maintainer to notify owner/licensee	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Data Maintainer to notify individuals								YL																														
Electronic notice allowed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Substitute notice allowed	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	YL	

Information compiled February 2016	Alaska Statute s45.48.010	Arizona s44-7501	Arkansas Code 1987 4-7-110	California Civil Code SB1386	Colorado Revised Statutes s6-1-716	Connecticut General Statutes s36a-701b	Delaware Code s12B	Florida Statutes s501.171	Georgia Code s10-1-910-915	Hawaii Civil Code 11-4-487N-1	Idaho Statutes 21-51	Illinois Compiled Statutes 815 ILCS 530/5	Indiana Code s24-4.9	Iowa Code 715C	Kansas Statutes 50-7a	Kentucky Revised Statutes 365.732	Louisiana Revised Statutes Title 51	Maine Revised Statutes s1347	Maryland Code 14-35	Massachusetts General Laws s93H-1	Michigan Identity Theft Protection Act	Minnesota Statutes 325E	Mississippi Code s75-24-29	Montana Code 2-6-15	Nevada Revised Statutes s603A	New Hampshire Revised Statutes 359C	New Jersey Statutes s56:8-161	New York Consolidated Laws 899-AA & 209	North Carolina General statutes 75-2A	North Dakota Century Code 51-30	Oregon Revised Statutes 14-646A	Pennsylvania Statute Title 73 Chapter 43	Rhode Island 11-49.3-2	South Carolina Code 30-1-90	Tennessee Code 47-18-21	Texas Code s521.002	Utah Code s13-44	Vermont Statutes 2430	Virginia Code s18.2-186.6	Washington Code 19-255-010	West Virginia Code s46A-2A	Wisconsin Statutes s134.98
Set time period to notify individuals								Y																							Y					Y		Y		Y
Safeguarding of information required								Y					Y											YL	Y						Y			Y	Y				
Internal policy deemed in compliance w/ law		Y			Y	Y	Y		Y		Y	Y	Y	YL	Y	Y	Y				Y	Y	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y		Y	Y	Y	
Specific monetary penalties outlined	Y			Y				Y		Y	Y			Y				Y	y		Y							Y					Y	Y	Y	Y	Y			Y	
Security credit freezes	Y				Y				Y																				Y		Y									
Best practice security program			Y	Y						Y									Y					YL				YL												
Data destruction and disposal			Y	Y				Y		Y		Y	Y		Y	Y								Y	Y		Y									Y	Y	Y			
Register of notifications to be maintained																			YL																					
Report to Governor/ Attorney General						Y					Y								Y	Y				Y				YL	YL	YL	YL						Y	Y	YL		
Report to Legislature										Y		YL																												
Report to Consumer reporting agencies	YL				YL			YL	YL			YL	YL		YL	YL		YL	YL		YL	YL		YL	YL	YL	YL	YL	YL	YL	YL	YL		YL	YL		YL	YL		YL	YL
Requirements for contents of notification				Y				Y		Y		Y		Y					Y	Y	Y					Y		Y	Y	Y	Y		Y				Y		Y	Y	