Law Council
OF AUSTRALIA

Exposure draft – Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

Attorney-General's Department

4 March 2016

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Acknowledgement

The Law Council acknowledges the assistance of its Business Law Section's Privacy Law Committee, the National Criminal Law Committee, and the Law Institute of Victoria in the preparation of this submission. The Law Council is also grateful for the opportunity to consult with the Commonwealth Attorney-General's Department during the preparation of this submission.

Executive Summary

1. The Law Council is pleased to provide the following submission to the Attorney-General's Department on the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (**the Bill**) and accompanying Mandatory Data Breach Notification Discussion Paper (**Discussion Paper**).

2. If enacted, the Bill would require Government agencies and businesses subject to the *Privacy Act 1988* (Cth) (**Act**) to notify the Office of the Australian Information Commissioner (**OAIC**) and affected individuals following a serious data breach.

3. Subject to the amendments outlined in this submission, the Law Council supports the passage of the Bill as a mechanism which would allow individuals whose personal information has been compromised in a serious data breach to take remedial steps to avoid potential adverse consequences.

4. The recommendations in this submission are further aimed at strengthening the Bill's safeguards, clarity, transparency and oversight mechanisms.

Introduction

5. The Australian Law Reform Commission (**ALRC**) in its 2008 report on privacy, *For Your Information: Australian Privacy Law and Practice* recommended introducing a mandatory data breach notification scheme on the basis that:

> *Data breach notification can serve to protect the personal information from any further exposure or misuse, and encourages agencies and organisations to be transparent about their information-handling practices.* [1]

6. The ALRC recommended that the Act be amended to impose a mandatory obligation to notify the Privacy Commissioner (**Commissioner**) and affected individuals where a data breach of personal information could give rise to a 'real risk of serious harm' to affected individuals.[2] Failure to notify would attract a civil penalty.[3]

7. In its 2013 report, the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) recommended in relation to mandatory data retention that any legislation include 'a robust, mandatory data breach notification scheme'.[4] The PJCIS subsequently recommended the introduction of a mandatory data breach notification scheme by the end of 2015 as a key safeguard to the mandatory data retention legislation.[5]

8. The Law Council agrees with the assessment of the ALRC and the PJCIS and supports the passage of the Bill, subject to addressing the concerns listed below.

Commencement date

9. In common with much legislation, the proposed Bill would commence on a single day (not more than 12 months from Royal Assent) to be fixed by proclamation, and in the absence of proclamation, on the anniversary of Royal Assent. The day on which Royal Assent of a Bill which has been passed by both houses of Parliament appears to follow no predictable pattern.

10. The Law Council offers no view on whether 12 months is an adequate timeframe for APP entities generally to develop systems and procedures to respond to the Bill, assuming it becomes law, but suspects that many entities would favour a longer period. The following submission continues on the basis that an implementation period in the order of 12 months is desired by the Government.

11. The Bill will implement new obligations affecting almost all non-small business organisations and agencies in Australia. Not only must there be an adequate period provided for implementation (after the final text of the Bill has passed the Parliament and all relevant regulations have been made and promulgated), but it would be useful

[1] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 1687-88, Recommendation 51-1.
[2] Ibid.
[3] Ibid.
[4] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) 192.
[5] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) Recommendation 38.

to ensure as far as practical that the obligations do not commence at an especially inconvenient time.

12. The Law Council notes that the *Privacy Amendment (Private Sector) Act 2000* (Cth) commenced on 21 December 2001 – the last trading Saturday before Christmas Day and the busiest day of the year for the retail trade – simply because the relevant Bill was conveyed to Government House on Thursday 21 December 2000, having passed the Parliament 14 days earlier on the last sitting day of 2000, 7 December.[6] The Law Council submits that it would be practical for the Government, as a red-tape reduction measure, to manage better the commencement date for legislation having a broad effect.

13. The Law Council suggests that the legislation should provide for a 'window' of between 12 months and 18 months from the date of Royal Assent, and that a date during that 'window' be expressly selected for proclamation. Such a date should be selected promptly after Royal Assent, in consultation with industry, with a view to minimising inconvenience due to public holidays, reporting periods, banking industry 'blackout' periods, or other seasonal factors which could increase the burden.

Recommendation:

- **The legislation should not automatically commence on the Anniversary of Royal Assent. A day between 12 months and 18 months after Royal Assent should be selected – promptly after Royal Assent – in consultation with industry organisations.**

Scope of the Bill and reference to 'other information'

14. Section 26WA of the Bill would provide that a new statutorily defined event called a 'serious data breach' occurs if there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (or certain other information) held by an entity and, as a result, there is a potentially quite remote risk (called a 'real risk') of serious harm to any of the individuals to whom the information relates.

15. A serious data breach would also occur if there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (or certain other information) held by an entity, and, any of the information is of a kind specified in the regulations.

16. The Act regulates 'personal information' as defined by section 6 of the Act. The term 'other information' is not defined and creates ambiguity about the scope of its obligations under the Bill. Unless that information in question is 'personal information', as defined, it would fall outside the scope of regulation under the Act and the powers granted to the Commissioner to administer the Act and the regime more broadly. References to 'other information' must be removed to preserve the existing regulatory structure and remain within the scope of the Act. We note that the scope of the

[6] For a more recent example, the *Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2016* (Cth) passed both houses on 20 October 2015, received Royal Assent 23 days later and will commence on a Saturday, 12 November 2016, during the financial sector 'blackout' period for technology changes.

definition of 'personal information', has been the subject of a Determination by the Commissioner and the matter remains contentious.[7] It would be unhelpful to further complicate this definitional issue.

Recommendation:

- **The term 'other information' in section 26WA of the Bill should be removed.**

Use of emotive language in key definitions

17. The name of the new statutorily defined event as a 'serious data breach' should be reconsidered, particularly as the criteria for the existence of a 'serious data breach' is determined on a probabilistic base where in many cases there will not in fact be any substantive interference with privacy, or that (in the case of a privacy breach with adverse consequences) not all potentially affected individuals would suffer any serious consequences. We submit that the phrase 'serious data breach' of itself has a heavy emotional weight. If such a defined term is used, the notices that affected APP entities must issue, and pronouncements of the OAIC, will automatically create an impression in any audience that some particularly 'serious' matter has occurred.

18. To avoid unnecessary alarm and unnecessary harm to the reputation of APP entities which appropriately assess relevant risks, the Law Council strongly submits that more qualified language should be used in the defined term. Without wishing to add significantly to the word length of notifications, the Law Council suggests that the phrase 'potentially serious data breach' would be a more accurate description and less likely to promote undue alarm.

Recommendation:

- **The defined term 'serious data breach' should be replaced wherever appearing by the term 'potentially serious data breach'.**

Delegation of legislative power – determination of important matters by regulation

19. Section 26WA of the Bill provides that a serious data breach also occurs if there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (or certain other information) held by an entity, and, any of the information is of a kind specified in the regulations.

20. Paragraph 26WB(2)(a)(ii) provides that a serious data breach will occur in situations where unauthorised access to or unauthorised disclosure of information of a kind referred to in new subsection 26WB(1) occurs, and any of the information is of a kind specified in the regulations. If subparagraph 26WB(2)(a)(ii) applies, unauthorised access to or unauthorised disclosure of information specified in the regulations is taken to be a serious data breach regardless of the risk of harm to individuals.

[7] *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015). The Law Council understands that this decision is the subject of impending judicial review.

21. The Explanatory Memorandum states the rationale behind this amendment:

> *This is intended to provide the flexibility to deal with data breaches that may not reach the threshold of a real risk of serious harm, but should nevertheless be subject to notification. These could include data breaches involving particularly sensitive information such as health records, which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection*.[8]

22. The kinds of information that should be subject to notification are integral as they determine the scope of the Bill's application. This concern is magnified if steps are taken to expand the scope of the regulation to apply to 'other information'. Given that the scope of the Act[9] is confined to 'personal information' as defined, any regulation that purports to extend to 'other information' that is not personal information, would be ultra-vires.

23. Given the breadth of the power to prescribe information, it is unclear why such a power is necessary. It is unclear how the example given in the Explanatory Memorandum regarding health records justifies this power, particularly as mandatory data breach notification is already required in the event of unauthorised access to eHealth information under the *My Health Records Act 2012* (Cth). In the absence of further explanation as to why this integral matter is proposed to be dealt with in the regulations as opposed to the primary legislation, the Law Council does not support this proposed amendment.

Recommendation:

- **In the absence of evidence to suggest otherwise, the kind of information that should be subject to notification which is integral in determining the scope of the Bill's application should be dealt with in the primary legislation as opposed to regulations.**

Scope of the regulation making power does not allow the specification of relevant circumstances

24. If, despite the Law Council's concerns expressed above, it is determined that it is appropriate for certain events to be prescribed by regulation as 'serious data breaches', the regulation making power should be expressed differently.

25. As drafted, any regulation would have the effect that any circumstance where unauthorised access to, or loss of, data '***may***' occur would automatically be a 'serious data breach' if the data included – to any extent – data of the prescribed kind. In our submission, such a power would not permit the drafter of the regulation to craft a regulation that properly deals with areas of concern.

26. For an effective regulation making power, a regulation should provide for kinds of information, and also ***circumstances*** relating to the potential for access or loss of the

[8] Explanatory Memorandum to the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, 12.
[9] Save for limited circumstances dealing with some provisions in Part IIIA of the Act dealing with de-identified data, such as section 20M.

relevant information. These might include for example, that actual loss of unencrypted information had occurred, or that unauthorised access was known to have occurred.

Recommendation:

- **If the clause 26WB(2)(c) regulation making power is adopted, a relevant regulation should provide both for kinds of information and specific circumstances in relation to the defined class of information.**

Any regulation making power should be able to conditionally exclude classes of potential data breach

27. The Bill does not include any mechanism under which particular circumstances which may technically involve a data breach but do not raise any serious consequences for individuals may be excluded from the reporting obligation on a class basis.

28. As a hypothetical example which is anecdotally not uncommon, assume that a sales representative changes employment and (against the policies of the former employer) takes with them a client list for use in their new role. Such an event would clearly involve unauthorised access, from the point of view of the former employer, but may be viewed with unconcern by the individuals affected.

29. To avoid unnecessary work by APP entities and by the OAIC, it would be useful to provide a mechanism to declare that specified kinds of events in specified circumstances are taken to not be 'serious data breaches'.

Recommendation:

- **Any regulation making power should allow specified circumstances to be conditionally excluded from being 'serious data breaches'.**

Any regulation making power should be required to be subject to transparent processes

30. If, despite the Law Council's concerns expressed above, it is determined that it is appropriate for certain events to be prescribed by regulation as 'serious data breaches', the exercise of the regulation making power should be subject to controls to ensure that the powers are exercised transparently and only where necessary.

31. The Law Council submits that the Bill should prescribe that a public consultation process with a comment period of at least 60 days should be required before the making of any regulation for the purposes of the Bill, and that a full privacy impact assessment and economic modelling of any proposed regulation should be required, to be carried out and published before the commencement of such public consultation period.

Recommendation:

- **The Bill should prescribe a process for open and effective public consultation in advance of the making of any regulation (in particular a regulation changing the characterisation of an event that would not be a 'serious data breach' under clauses 26WB(2)(a)-(b)).**

Types of breaches that are reportable

32. One key area of improvement under the new Bill is the greater emphasis placed on establishing 'reasonable grounds' for determining that a 'serious data breach' has occurred before deciding to notify. This is an issue of critical importance, as it marks the line between notifiable and non-notifiable breaches.

33. Accurate information can be difficult to come by in the immediate aftermath of a data breach incident, and assessments of the scale and severity of a data breach incident often evolve rapidly as new information becomes available.

34. There are significant potential pitfalls for entities in choosing to notify individuals or publicising information before the entity has the full picture. In light of this, the introduction of an 'assessment period' to allow the entity to more fully investigate the breach seems sensible.

35. It's interesting to note that, under the current drafting, the Commissioner needs to be satisfied that 'reasonable grounds' exist before s/he can assert that the notification obligation applies. It's not yet entirely clear how the Commissioner will apply this requirement when reviewing an entity's handling of a data breach incident, given that risk assessments are often conducted under time pressure and with limited information.

Risk

36. Section 26WG would provide that, for the purposes of the new Part IIIC, the term 'real risk' means a 'risk that is not a remote risk'. It is difficult to apply a double negative to a positive obligation (in this case to notify).

37. The Law Council is concerned by the selection of what might be seen as an inherently subjective test as a matter that is essential to the identification of a 'serious data breach', particularly as clause 26WB(2) primarily requires the consideration of matters going to the seriousness of harm rather than the level of confidence that any harm would be likely to actually occur.

38. In particular it is far from clear how a possibility objectively assessed as 1 in 100, or 1 in 50, should be assessed under the proposed 'not remote' test. To express this another way, would a risk assessed as 'highly unlikely' be assessed as 'remote' or 'not remote'? The Law Council is unable to judge this, and submits that affected organisations also will be unable to do so. For completeness, the Law Council also notes that in a number of risk related fields, attempts have been made to quantify risk

descriptions and provide for an element of consistency.[10] Serious consideration should be given to streamlining description of data breach related risks and likely impacts.

Recommendation:

- **Replace the 'not a remote risk' double negative test with a positive test, such as 'real risk', 'likely risk' or 'probable risk'.**

Relevant matters

39. New subsection 26WB(3) would provide a non-exhaustive list of relevant matters entities must have regard to when determining whether a real risk of harm exists. It is important and necessary to keep these matters technology-neutral as a way of preventing obsolescence. For example, the reference to encryption may need to be 'encryption, other forms of protections, controls or tools applied by the entity or their respective service provider (if any)'. This would include for example passwords and cover cloud service providers.

Recommendation:

- **The list of relevant matters should be more generic, for example, reference to encryption should be amended to read 'encryption, other forms of protections, controls or tools applied by the entity or their respective service provider (if any)', or a defined term such as 'adequate technological protections' should be used.**

Report to the Privacy Commissioner

40. New subsection 26WC(1) provides that if an entity is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity (as defined in new section 26WB), the entity must, as soon as practicable after the entity becomes aware, or ought reasonably to have become so aware:

ANTHONY G. PATT AND DANIEL P. SCHRAG

Table I
IPCC qualitative descriptors

Probability range	Descriptive term
< 1%	Extremely unlikely
1–10%	Very unlikely
10–33%	Unlikely
33–66%	Medium likelihood
66–90%	Likely
90–99%	Very likely
> 99%	Virtually certain

10 Table from Anthony Patt and Daniel Schrag, 'Using Specific Language to Describe Risk and Probability' *Climate Change* (2003) 61: 17-30.

- prepare a statement that complies with new subsection 26WC(3) (paragraph 26WC(1)(a)); and

- give a copy of the paragraph 26WC(1)(a) statement to the Commissioner.

41. The items listed in subsection 26WC(3) generally would be construed as admission of liability or evidence. It would be useful if the notice was 'without prejudice' or issued on a 'no admission of liability' basis. This is because the notice may describe matters that may or may not lead to harm and of itself be a form of mitigation or steps towards it. Making it clear that the notice itself is not an admission would support and encourage transparency and accountability by the entity or entities involved. It would not deprive the Commissioner of the powers to investigate and draw conclusions based on the evidence in a given incident.

Recommendation:

- **The Bill should be amended to clarify that a notice given under subsection 26WC does not constitute an admission of liability by the entity giving the notice.**

Harm

42. Section 26WF would provide that, for the purposes of the new Part IIIC (notification of serious data breaches), the word 'harm' includes physical harm, psychological harm, emotional harm, harm to reputation, economic harm, and financial harm. This is a non-exhaustive list.

43. Harm would include the additional items of physical harm, psychological harm, emotional harm and harm to reputation.

44. The system may be easier to administer if the concept of harm was not so specific to this regime. The Law Council notes that the Act refers to loss or damage for certain types of matter which may attract compensation under the Act.[11] For example the Commissioner has power to make a determination that deals with:

    - 'conduct to redress any *loss or damage* suffered by the complainant';[12] or

    - compensation for any *loss or damage* suffered by reason of the act or practice the subject of the complaint'.[13]

45. Subsection 52 (1AB) of the Act provides that: the loss or damage referred to in paragraph (1)(b) or subsection (1A) includes:

    (a) injury to the feelings of the complainant or individual; and

    (b) humiliation suffered by the complainant or individual.

2. The definition of harm as defined in the Bill does not align to the above concepts.

[11] *Privacy Act 1988* (Cth) s52.
[12] Ibid, s52(1)ii.
[13] Ibid, s52(1)iii.

Recommendation:

- **The current definition of harm should be removed and replaced with a reference to the types *loss or damage* as covered by the *Privacy Act 1988* (Cth), namely the matters that fall within the Privacy Commissioner's powers pursuant to section 52 of the Act.**

Timing obligations

Ought reasonably to have become aware

3. New subsection 26WC(1) provides that if an entity is aware, or 'ought reasonably to be aware', that there are reasonable grounds to believe that there has been a serious data breach of the entity, the entity must, as soon as practicable after the entity becomes aware, or ought reasonably to have become so aware notify the Privacy Commissioner.

4. The language of 'ought reasonably to have become aware' is too broad and uncertain. Given that the Bill imposes a positive obligation with a relatively short time period to take action, breach of which carries a substantial sanction, the test needs to be more certain. The Law Council notes that in the course of the consultation process with the Attorney-General's Department, the Department was clear that the Bill is not intended to extend the existing obligations under Australian Privacy Principle (**APP**) 11. Language based on the existing compliance standard as expressed in APP 11 would be more appropriate.

5. The Law Council also notes that APP 11 and the Act itself applies to the information that the entity holds. A test that focuses on information that an entity 'ought reasonably to be aware' is at odds with the concept that the entity is accountable for the information that it holds, as defined by the Act.[14]

Recommendation:

- **The scope of the timing obligation should be narrowed by:**
  - **removing a reference to 'ought reasonably be aware' entirely; or**
  - **replacing it with a reference to if 'reasonable steps were taken to ensure security of personal information, the entity would have been aware' or a similar formulation that aligns with APP 11.**

Standard of corporate awareness

6. Commonly under the Act, the regulated APP entity will be an organisation (such as a corporation) which acts through a variety of individuals. The Law Council submits that it is not clear whether an APP entity would be taken to be 'aware' of particular circumstances when two or more of its personnel collectively have knowledge of all of

[14] Section 6 of the Act provides that 'an entity holds personal information if the entity has possession or control of a record that contains personal information'.

the circumstances that could cause knowledge of a serious data breach, but no individual knows all of the information that would cause them to know of the serious data breach.

7. Following considerable debate as the final form of legislation was developed, the suspicious matter reporting obligation in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) may be a more suitable basis. That Act specifies a short time limit to start only when a 'reporting entity' in fact forms a relevant suspicion, not at an earlier time when it (or one or more of its personnel) know relevant facts which could form the basis of a suspicion.

8. It should be clarified that an APP entity's awareness of a serious data breach does not happen before the time that an employee or officer of appropriate seniority is actually aware of the likelihood of a serious data breach.

Recommendation:

- **The Bill should clarify that for the purposes of section 26WC(1), an organisation is not aware of a serious data breach until an appropriate officer actually suspects the existence of a serious data breach.**

30 day time limit

9. Where an entity is uncertain as to whether there are reasonable grounds to believe a serious data breach has occurred, new subsection 26WC(2) would provide that the entity has 30 days to reasonably assess whether there are such reasonable grounds before the entity is required to notify the Commissioner and affected individuals.

10. The 30 day time limit may not be sufficient time to allow an entity to undertake a detailed forensic assessment to determine the significance of the data breach. While it is important to ensure that a serious data breach is notified to the Commissioner in a timely way, to ensure that serious data breaches are reported, it would be useful if there was provision for an entity to apply to the Commissioner for an extension of time for 30 days or such other time as determined by the Privacy Commissioner.

Recommendation:

- **The Bill should be amended to expressly empower the Commissioner, on application by an APP entity to extend the 26WC(1)(c) and (d) period by 30 days or such other time as determined by the Commissioner, for the purpose of the APP entity reasonably assessing whether a serious data breach has occurred.**

Overlap with other mandatory notification requirements

11. In a number of regulated industries (such as health or financial services), entities have industry specific breach notification requirements to their respective regulators, such as the Australian Securities and Investments Commission or the Australian Prudential

Regulatory Authority. The reporting provisions in the Bill may cut across a number of these.

12. It would be helpful to clarify that where an entity has notified a relevant regulator or an affected individual they are taken to have complied with the provisions under the Bill.

13. Similarly, where there are multiple parties involved and one party notifies (for example, a service provider, doing so, pursuant to a contract requiring them to do so), that should remove a corresponding need for another party (an entity that also holds the personal information) to notify the Commissioner or the affected individual or individuals. This will be important to avoid multiple and potentially unnecessary notifications in circumstances where there are multiple service providers or a chain of data holders (for example, in outsourcing arrangements or credit reporting environments).

14. In this context, the Law Council notes that the definition of 'hold' in section 6 of the Act, includes possession or control, and assumes an environment of multiple entities that are capable of holding the same personal information at the same time and hence being subject to obligations under the Act.

Recommendations:

- **In relation to an existing duty to notify, add an additional exception that applies to existing mandatory notification provisions applicable to financial services, telecommunications and health service providers, where such a notification was so made.**

- **In relation to a data breach involving multiple parties who have possession or control of the relevant personal information and one party is contractually bound to make the notification under the Bill, the notification by that party will be taken to have been by all the other entities who 'hold' the personal information in question at the time of the serious data breach.**

Law enforcement exception

15. In recommending a mandatory data breach notification scheme in 2008, the ALRC also recommended that the Privacy Commissioner could waive notification requirements where it would be in the public interest.[15] The ALRC noted that this:

> *… would cover situations, for example, where there is a law enforcement investigation being undertaken into the breach and notification would impede that investigation, or where the information concerned matters of national security*.[16]

16. Unlike the ALRC's recommendation, new subsection 26WC(5) of the Bill would allow the relevant entity who is a law enforcement body not to notify affected individuals where the body believes on reasonable grounds that compliance with paragraphs 26WC(1)(c), 26WC(1)(d) and 26WC(3)(d) would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body.

[15] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 1693, Recommendation 51-1.
[16] Ibid.

17. The entity must still notify the Commissioner (with the exception of paragraph 26WB(3)(d)), which is a welcome initiative to enable the Commissioner to assist law enforcement bodies in responding to the serious data breach.

18. However, transparency and accountability are needed around a decision by a law enforcement body under subsection 26WC of the Bill not to notify affected individuals where the body believes on reasonable grounds that compliance would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body. The Privacy Commissioner is not empowered to offer scrutiny of such decisions.

19. The Commonwealth Ombudsman, who has oversight of the data retention regime for law enforcement bodies, is well-placed to have independent oversight of the exercise of law enforcement agencies' exercise of powers under subsection 26WC(5) of the Bill. To enhance oversight and public confidence in the proposed exception, the Law Council recommends that the exception be subject to annual reporting to the Parliament and appropriate oversight by the Commonwealth Ombudsman.

Recommendations:

- **The Bill be amended to require a law enforcement body to notify the Commonwealth Ombudsman as soon as practicable following a decision not to notify an affected individual of a serious data breach under subsection 26WC(5) of the Bill.**

- **The Bill be amended to require the Commonwealth Ombudsman to report annually regarding law enforcement body exceptions to notification. The matters to be included in the report should include the number of instances where individuals were not notified of a serious data breach, and the appropriateness of the law enforcement body reaching a determination not to notify an affected individual.**

Exception – Commissioner's notice in the public interest

20. Similarly, if law enforcement bodies or intelligence agencies are to provide private sector organisations, Commonwealth agencies or the Privacy Commissioner with advice that notification to affected individuals might impede a law enforcement investigation or that the information concerns matters of national security and hence may not be in the public interest under subsections 26WC(6) and (7) of the Bill, the appropriateness of that advice should be subject to adequate independent scrutiny.

Recommendations:

- **The Bill be amended to require a law enforcement body or an Australian intelligence agency to notify the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security (IGIS) (respectively) as soon as practicable following a decision to advise a relevant entity or the Privacy Commissioner that notification of a serious data breach might impede a law enforcement investigation or that the information concerns matters of national security.**

- **The Bill be amended to require the Commonwealth Ombudsman and the IGIS to report annually regarding the number of instances where a law enforcement body or intelligence agency has provided such advice, and to report on the appropriateness of such advice.**

Legal Privilege

21. It is highly likely that entities will seek legal advice about their duties under this Bill. This is particularly so as the threshold issues as to the very existence of a type of harm or type of risk that arises requires consideration of the new definitions created and in the possible context of multiple assessments (such as IT and forensics). It is important that the legal advice properly sought in the course of a crisis does not erode legal privilege.

22. The Law Council appreciates that privilege cannot be eroded unless it is expressly removed. However, the extent to which it applies could be clarified in the Explanatory Memorandum and relevant guidance.

Recommendation:

- **Consider making the extent to which legal professional privilege applies clear in the Explanatory Memorandum and relevant guidance.**

Resourcing

23. The OAIC must be appropriately funded and resourced in order in order to properly oversee the data breach notification scheme. In 2013, the OAIC noted…

> *…implementation of the provisions of the [Privacy Amendment (Privacy Alerts)] Bill will have a significant impact on the OAIC's workload and resources. The OAIC will need to modify its existing workflow and document management systems to deal with the nature and volume of the notifications that will be required by the Bill; this will result in an increase in the OAIC's capital cost.*[17]

[17] Professor John McMillian, Australian Information Commissioner, Timothy Pilgrim, Australian Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee's Inquiry into Privacy Amendment (Privacy Alerts) Bill 2013* (2013) 6.

24. Sufficient budget provisions are needed to ensure the OAIC is able to effectively perform its legislative functions. The Law Institute of Victoria (LIV) has also stated that the Government should also provide greater certainty for the OAIC by appointing a Privacy and Freedom of Information Commissioner.

Recommendation:

- **Appropriate funding and resourcing should be provided to the Office of the Australian Information Commissioner.**

Draft guidelines

25. The Privacy Commissioner will have the discretion to issue guidelines under paragraph 28(1)(a) of the Act about matters relating to compliance with the new Part IIIC—Notification of serious data breaches.

26. An exposure draft of any guidelines that are proposed to be issued by the OAIC to provide clarity to APP entities on the operation of the new mandatory notification requirements should be developed in consultation with relevant stakeholders. The Law Council would not be adverse to industry specific guidance being issued given the different issues that may arise for various sectors. It would be willing to work with the OAIC in the development of such guidelines, should it assist.

Recommendation:

- **An exposure draft of any guidelines that are proposed to be issued by the OAIC to provide clarity to APP entities on the operation of the new mandatory notification requirements should be developed in consultation with relevant stakeholders. Consideration should be given to the development of industry specific guidance**.

Alternate views

27. The LIV has raised alternate views relating to the 'real risk of serious harm' threshold and the secrecy exception. These alternate views are set out below for the Attorney-General's Department's consideration.

28. The LIV has recommended that the 'real risk of serious harm' threshold should be lowered.

29. The LIV notes that the 'real risk of serious harm' threshold has been considered and recommended by the ALRC, and is adopted in the OAIC's *Data Breach Notification — A guide to handling personal information security breaches.*

30. Further, the LIV notes that some organisations (such as the Australian Privacy Foundation and Liberty Victoria) have argued that any breach should be subject to notification when there is any risk of harm.

31. The LIV recommends that 'real risk of serious harm' threshold be lowered to include any form of harm. This is critical because the magnitude of privacy risks is generally

cumulative, not individual, that is, small risks to a number of people. The consequences of that small risk to an individual can be significant.

32. Determinations as to whether harm exists require consideration of factors known only to the victims and, accordingly the LIV recommends that a cautious approach be taken.

33. The LIV further recommends that a conservative approach be adopted when determining the level of risk. It is difficult for an entity to ascertain the level of risk when this is dependent on the future actions of the person who has accessed the data. The LIV therefore considers that the 'real risk' threshold be lowered.

34. The LIV is currently exploring alternative wording for the threshold test and would appreciate the opportunity for further discussion with the Attorney-General's Department on this point, as the consultation progresses.

35. The LIV has also expressed the view that the secrecy exception is not a necessary inclusion in the Draft Bill.

36. The LIV queries the necessity of including the secrecy exception in the Draft Bill, given that the scheme will not apply where secrecy provisions in other legislation already apply, one example being with respect to national security.

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2016 Executive as at 1 January 2016 are:

- Mr S. Stuart Clark AM, President
- Ms Fiona McLeod SC, President-Elect
- Mr Morry Bailes, Treasurer
- Mr Arthur Moses SC, Executive Member
- Mr Konrad de Kerloy, Executive Member
- Mr Michael Fitzgerald, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.