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)*	Boon Poh Mok Director, Policy - APAC BSA | The Software Alliance
Contact details *(one or all of the following: postal address, email address or phone number)*	Email: [redacted]

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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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

--- PLEASE TURN TO NEXT PAGE ---

4th March 2016

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

Dear sir / madam,

RE: BSA COMMENTS ON THE EXPOSURE DRAFT OF THE PRIVACY AMENDMENT (NOTIFICATION OF SERIOUS DATA BREACHES) BILL 2015

BSA | The Software Alliance[1] welcomes this opportunity to comment on the exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill) proposed by the Commercial and Administrative Law Branch of the Australia Attorney-General's Department.

BSA members have made significant investments in Australia and proud that many Australian companies, organizations, and consumers continue to rely on BSA member products and services to support Australia's economy. While BSA is supportive of the Government's goals to improve the privacy of Australians without placing unreasonable regulatory burdens on businesses, we remain concerned that the Australia Government is departing from international best practices by creating a new breach notification regime which imposes additional burdens to businesses in Australia without increasing cybersecurity. BSA would like to provide the following comments and recommendations over several concerning proposed provisions in the exposure draft.

Definition of "serious data breach"

Notification should not be mandatory where there is no real risk of serious harm. The proposed sections 26WB(2)(a)(ii) and 26WB(2)(c) provide that a serious data breach occurs even where there is no real risk of serious harm.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro and Workday.

BSA believes that notification should always depend on the existence of a real risk of serious harm, otherwise 'notification fatigue' may result, wherein individuals are notified of data breaches when no serious harm is likely to occur from those breaches, and become unduly inconvenienced or fail to take appropriate action in response to those notifications where there is a real risk of serious harm.

BSA favours the introduction of a breach notification system that helps incentivise entities to ensure robust protection for personal data, while enabling data subjects to take action to protect themselves in the event their data is compromised. Any proposal should, however, be carefully crafted to prevent the issuance of immaterial notices, principally by ensuring that notice is only required where there is a serious risk of harm to the user and by excluding from the notice obligation data that has been rendered unusable, unreadable or indecipherable to an unauthorised third party through practices or methods, such as encryption, redaction, access controls or other such practices or methods, which are widely accepted as effective industry practices or industry standards. This model, introduced in the EU with the ePrivacy Directive for electronic communications services has recently been extended to all businesses and organisations under the General Data Protection Regulation.

BSA presumes that the purpose of these provisions is to allow the Attorney-General to prescribe some categories of personal information as so sensitive that any breach should be notified. This is not a feature of most notification laws in other jurisdictions, and BSA believes that it should always be possible to assess whether a real risk of serious harm arises from a given incident. For these reasons, BSA submits that proposed sections 26WB(2)(a)(ii) and 26WB(2)(c) should be deleted from the Bill.

Furthermore, Section 26WF of the proposed Bill extends "serious harm" to broadly include physical, psychological, emotional and reputational harms. These elements of the "serious harm" definition could be subjective. BSA is of the opinion that "serious harm" should be narrowly and objectively defined to avoid diverging interpretations and legal uncertainty.

Contractors versus principals

Unlike other jurisdictions, the Australian legislation does not distinguish between contractors (i.e. data processors) and principals (i.e. data controllers). Proposed section 26WC(1) requires the entity to which the serious data breach has occurred to issue the notices. However, with the increasing growth of the cloud IT services market, in many cases the entity that is holding or processing the relevant information is a contractor of the principal entity that has the relationship with, and collected the personal information from, the individuals to whom the relevant information relates. Indeed, in many cases the contractor may not know the individuals to whom the information relates, as they merely passively hold or process that information on behalf of the principal.

BSA believes that it is more appropriate and efficient for the principal to be responsible for issuing the notice to the affected individuals, rather than the contractor. The obligation of a contractor should be to notify its principals when a serious data breach occurs in respect of the contractor, and the obligation of the principals should be to then provide the relevant notices to individuals that are

affected. In addition, the obligations of the Bill should attach to principals that have an Australian link (including data breaches by its offshore contractors), and not contractors themselves that have no Australian link. This is consistent with proposed section 26WB(5) in relation to overseas recipients.

BSA also notes this would be consistent with the spirit of proposed section 26WC(4), as a contractor likely does not have a normal mode of communication with the individual data subjects, where the principal likely does. BSA considers this provision to be consistent with global best practices.

BSA further notes that placing the primary responsibility on the principal, for notifying affected individuals of serious data breaches, is also consistent with how the Office of the Australian Information Commissioner ("OAIC") considers APP entities (as defined in the *Privacy Act 1988*), in certain instances, as still being the primary entities responsible for any mishandling of information and the consequent breach of the Australian Privacy Principles ("APPs") even though mishandling may have occurred while the information was in the contractor's physical possession[2].

In this regard, we feel that the distinction that the OAIC draws between when an APP entity is "using" vs when it is "disclosing" information, in relation to the operation of APP 8, should carry over to considerations of a breach notification. In other words, where the contractor (whether onshore or offshore) is receiving information from the principal "*for the limited purpose of performing the services of storing and ensuring the entity may access the personal information*…"[3], the principal should still be treated as the one "using" or "holding" the information and thus responsible for determining whether serious harm has occurred, and for notifying the relevant individuals accordingly. The contractor's responsibility in this instance should only be to notify the principal of the breach in accordance with the terms of their contract.

Definition of "as soon as practicable"

While BSA recognises the importance of promptness when notifying data subjects about a serious data breach that has occurred, we believe that the current drafting is overly strict. The current drafting in section 26WC(1) requires that the entity prepare its disclosure statement "as soon as practicable".

Section 26WC(2) provides that "as soon as practicable" includes the time taken by the entity in carrying out a reasonable assessment of whether there are reasonable grounds to believe the relevant circumstances amount to a serious data breach of the entity (provided that the assessment

---

[2] See the OAIC's guidelines on APP 8 – Cross-Border Disclosure of Personal Information (https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information). See, in particular paragraphs 8.14 and 8.15 of the guidelines, where the OAIC considers that the APP entity is still "using" the information, where the APP entity provides the information to a contractor "*for the limited purpose of performing the services of storing and ensuring the entity may access the personal information*", and a there is a binding contract between the entity and the contractor that (i) requires the provider only to handle the personal information for these limited purposes (ii) requires any subcontractors to agree to the same obligations; and (iii) gives the APP entity effective control of how the personal information is handled by the contractor.

[3] *Ibid.*

is performed within a certain amount of time). However, there are other activities that should also be given similar allowance is determining what is "as soon as practicable".

BSA believes that in the event of a serious data breach, the foremost priority for the affected entity should be stopping or containing the breach, and fixing the vulnerability or error that caused it. If containing the breach is left until after a notification is issued, the risk of harm arising from the breach would no doubt have increased.

BSA would encourage the Australian government to follow best practices that exist in other regions and should not create a new regime that is out of step with international systems. For instance, one emerging best practice is a two-step approach for breach notification:

a. Under these regimes, the controller should without undue delay after having become aware of the breach notify the personal data breach to the competent supervisory authority, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.

b. The individuals are solely notified if the personal data breach is likely to result in a significant risk of harm to individuals, in order to allow them to take the necessary precautions. The communication to the data subject is not be required if:

    i. appropriate technical and organisational protection measures were implemented and applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

    ii. subsequent measures to ensure that the significant risk of harm to data subjects is no longer likely to materialize have been taken by the controller; or

    iii. it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The Australian government should follow global best practices and should not create a new regime that is out of step with international breach notification systems.

Further to the points raised in section "**Contractors versus principals**" above, there should also be consideration of the time required for contractors to notify principals and the principals to then notify the relevant individuals.

BSA submits that these activities should also be expressly included in the scope of "as soon as practicable" under section 26WC(2).

Time for compliance runs from when entity "ought reasonably be aware"

The use of the phrase "ought reasonably to be aware" appears to be intended to avoid the possibility of wilful blindness from regulated entities (that is, entities deliberately not implementing protocols that would bring serious data breaches to their attention, so as to avoid being subject to the breach notification obligations). However, if an entity is genuinely unaware of a breach, it will automatically be unable to comply with proposed section 26WC(1) because it must act "as soon as practicable" after it "ought reasonably be aware of the breach", not when it actually became aware of the breach.

BSA notes that APP 11.1 requires that APP entities take such steps as are reasonable to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure. This obligation would no doubt include the installation of systems and protocols that bring to the entity's attention any actual or potential data breaches.

BSA believes that provided that a regulated entity is complying with APP 11, there is no need to include the phrase "ought reasonably be aware" in section 26WC(1). Its inclusion only introduces uncertainty and potentially means that an entity could institute controls consistent with APP 11, but due to events outside the entity's control the system did not detect a serious data breach when it occurred, and the entity subsequently would be in breach of section 26WC(1) when it had no way of knowing of the breach and was therefore incapable of complying.

If a regulated entity has breached APP 11.1 by failing to implement systems and protocols that notify the entity of actual or potential data breaches, and because of this the entity fails to notify the affected individuals, those individuals will have rights against the entity under the Privacy Act so there is little utility in imposing liability for a second "interference with the privacy of an individual" arising out of the same underlying conduct. Furthermore, given that breach notifications can appear to be admissions of liability, and may lead to class action litigation filed against the notifying party, it becomes even more important to ensure that notices are not required when they are not necessary.

BSA suggests that the words "or ought reasonably be aware" and "or ought reasonably have become so aware, as the case may be" be removed from the section or, in the alternative, an additional section added to the Act to clarify that where an APP entity has complied with APP 11.1 by taking reasonable steps to implement systems designed to detect serious data breaches, the entity ought reasonably to be aware that there has been a serious data breach (or that there are reasonable grounds to believe that there has been a serious data breach) only where those systems have detected the serious data breach (or detected the basis for the reasonable grounds to believe such a breach has occurred).

Exemption for compliance with law enforcement directions

Following a serious data breach, the affected entity may need to cooperate with law enforcement investigations relating to the breach. In addition to the exceptions set out in section 26WC(6) to 26WC(14), BSA proposes that an entity should not be required to issue a data breach notice in circumstances where an enforcement body advises the entity that such notice would prejudice the enforcement body's ongoing investigations or enforcement activities. BSA believes that entities

should not be put in the position where they must either breach their obligations under the Privacy Act or refuse to comply with a direction from a law enforcement agency.

BSA notes that under proposed section 26WC(5), enforcement bodies are exempt from notifying affected individuals (although they must still prepare the statement and provide it to the Commissioner) where the enforcement body reasonably believes that it would be likely to prejudice its enforcement activities. BSA believes that to the extent an enforcement body directs a non-enforcement body to take certain steps (including refraining from issuing a breach notice to affected individuals), that non-enforcement body should be entitled to at least the same exemption under section 26WC(5) as the enforcement body would be entitled to if it took those steps itself.

Under the proposed section 26WC(6), regulated entities can apply to the Commissioner for an exemption in such circumstances, and the Commissioner may exempt the entity if the Commissioner believes it is in the public interest to do so. This process is time-consuming and would require the Commissioner to second-guess the law enforcement agency's assessment of the likely impact of a notification on their activities.

In the alternative to an exception to the obligation to issue a data breach notice for compliance with directions of an enforcement body, the regulated entity should be permitted to issue a data breach notice after the conclusion of any law enforcement investigation or enforcement activities that would be prejudiced by the issuance of the notice, or the receipt by the regulated entity of a direction from the relevant law enforcement agency that the enforcement activities would no longer be jeopardised by the issuance of the notice.

BSA greatly appreciates the opportunity to provide these comments. We would be delighted to have further engagement with the Government of Australia to respond to any questions and to explore ways in which BSA and our members can work with the Government to achieve its goals.

Sincerely,

[redacted]

Boon Poh Mok
Director, Policy – APAC
BSA | The Software Alliance