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)*	Nicole Murdoch
Contact details *(one or all of the following: postal address, email address or phone number)*	[contact details 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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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? 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

Submission

1. I am an Electrical Engineer and a Senior Associate in the Intellectual Property practice division of Bennett & Philp Lawyers.

2. For approximately 10 years and before I entered the legal profession, I worked in the information technology sector and held roles within the encryption industry including as a security tester.

3. I have worked in the legal industry for approximately 9 years and as part of my current role I assist corporations and individuals in respect of information theft matters. From my experience in the IT sector and from my experience in IP law, I am in a position to understand both the challenges facing corporations in their attempts to go about their businesses whilst also protecting information against theft and also the effects that information theft has on individuals and corporations.

4. I mention my background and position to draw attention to my experience within the information protection, security and legal industry only. The opinions and views herein are my own and they may or may not align with those of my employer.

5. Within these submissions I reference the alleged unauthorised access to the database of a US entity. My references to that alleged access are based on reports and information

available to me in the public domain. I do not adopt those reports or the information within those reports as being my own and I cannot know the truth of the allegations surrounding that alleged breach, I simply report the issue by way of example.

Mandatory Notification Data Breach

6. I fully support the proposed mandatory requirement to report data breaches. However, as outlined in these submissions, I have some concerns with the wording and the discretionary nature of the notification requirements of the Privacy Amendment (Notification of Serious Data Breaches) Bill ("the Bill").

7. The Bill requires that an APP entity gives a notification of a serious data breach only if the breach *will result in a real risk of serious harm* to any of the individuals to whom the information relates.

Discretion of APP Entity

8. Under the Bill, notification of a breach is only a requirement if, in the opinion of the APP entity, the breach will result in the real risk of serious harm to any of the individuals to whom the information relates.

9. The decision of whether serious harm is a real possibility should not be at the discretion of the APP entity.

10. An APP entity cannot know all of the circumstances or mindset of an individual and it cannot know what harm an individual is likely to suffer if that individual's information is disclosed without authorisation. The opinion of an APP entity in that respect may not align with that of an individual. Even mere association of an individual with an APP entity may cause that individual serious harm.

11. It should also be kept in mind that the APP entity is likely to be embarrassed by the breach and thus has an interest in not reporting the notification. Data breaches have previously led to the failure of businesses and those factors will, even subconsciously, play a role in the decision making process of the APP entity.

12. I understand concern over notification fatigue, however, the choice of whether an individual chooses to ignore a notification or not should be left to the individual as it is that individual the suffers the consequence of the breach.

13. I submit that, it is appropriate for Australia to follow the European Model of mandatory breach notification and an APP entity should be required to make a notification following a data breach involving personal information regardless of the perceived level of risk to those affected.

Limitation to Individuals to which the Information Relates

14. The Bill requires that it is only necessary to notify of breaches where there is a real risk of serious harm to any of the individuals to whom the information relates. Thus unauthorised access to de-identified data would not fall under the mandatory notification requirements.

15. My concern in that regard lies with the potential to re-identify the data. Identification of individuals can occur through the interrogation or manipulation of multiple sub-sets of data not only one set of data. Given the prevalence of information available on individuals in the public domain the identification of an individual may occur even though the data obtained from an APP entity does not, in itself, include identifying data.

> To use an example, if an APP entity stores the last four digits of a credit card number, the initials of an individual and the purchase details of the individual, that data alone would not be sufficient to identify an individual. Thus the APP entity, under the Bill, would not be required to report the breach. However, if that data is then matched with a database containing the last four digits of a credit card number and the person's full name then a bad actor can confirm (through deduction) which individuals were involved in the data breach and identify their purchases.

16. Whether the data can be re-identified would clearly depend on the data involved but again the decision on whether to make a notification should not be left to the APP entity.

17. It is also perceivable that the breach may identify the possibility of real risk of harm, to individuals to whom the information does not relate.

> For example the breach may highlight a serious flaw in security measures, which if detected early enough, may result in protections being put in place to protect other individuals from bad actors taking advantage of the same security flaw.

Relevant Matters

18. The Bill lists relevant matters to which the APP entity should have regard when determining of there is a real risk of serious harm to an individual. Some of these matters include whether the information is in an intelligible form to an ordinary person, whether the information is protected by security measures and whether the entity has taken, is taking or will take steps to mitigate the harm.

19. Whilst it is understood that these matters are not exhaustive and are not determinative in themselves, the question of whether harm is likely to occur should never be answered by reference to whether the information is in an intelligible form to ordinary persons. Ordinary persons are not bad actors and they are not the persons who seek to re-identify or decrypt data for their own nefarious means. In any event:

    (a) decryption techniques are continually evolving and the decision on whether information can ultimately be decrypted should not be determined by an assessment of current decryption techniques; and
    (b) the risk of harm should not be assessed by whether harm will occur if the data is in the hands of ordinary persons as ordinary persons mean no harm.

20. The risk of serious harm may not be mitigated by steps taken by the APP entity. Mitigation techniques take time to implement and in that respect harm can occur immediately. It may be that mitigation by the entity can never fully mitigate the loss. The APP entity may stop the breach but data may have already been released and spread irretrievably around the world. Again the APP entity cannot know whether its techniques have or will mitigate harm.

Notification Requirements

21. Under 26WC of the Bill an entity must make the notification as soon as practicable after becoming aware of the breach. However, under ss 26WC(2) it can assess the matter for 30 days after becoming aware (or after it ought to become aware).

22. The 30 day period is far too long for the assessment and notification to occur. The first step in notification should be a notification (with as much information available at that time) of the breach. That first notification should occur with 48 hours of a data breach (or after the entity ought to become aware). Thus individuals can take immediate steps to mitigate their loss as they see fit. There should then be a further notification with more information that comes to hand. The further notification should be made within 7 days of the initial notification, with any further notifications as necessary. That process will allow individuals to mitigate their losses immediately rather than the individual having to wait up to 30 days to begin the mitigation process.

> To use an example, if an APP entity stores credit card details then the notification of the unauthorised release of that information will allow the individual to notify their credit provider of the breach immediately. If the person was not aware of the breach for 30 days then it is highly likely the credit card would have already been used resulting in harm not only to the individual but also to the credit provider.

23. Under the Bill, the notification does not need to be made publicly but only needs to be made to the Commissioner and the individual concerned. Whilst I understand that entities would not want the embarrassment associated with a notification and it is likely that major data breaches would be reported by the media, the general public should be put into a position where they can assess an entity's history of data breaches before engaging with that entity. Accordingly a public notification should be required.

24. I understand that entities should not be forced to make a notification if they only merely suspect that a breach may have occurred. However, there needs to be some middle ground between protection of information and individuals and the individual's ability to quickly mitigate loss and the ability of a business to go about its business without making

unnecessary notifications. Accordingly I support the statement that the notification only be made if there are "reasonable grounds to believe there has been a" breach.

Example uKnowKids

25. The importance of immediate notification in respect of unauthorised access of information has recently been highlight by a security breach involving software which assists with the protection of children.

26. uKnowKids is a US based platform by which parents and guardians can monitor and track their children.[1] Under my understanding, the uKnowKids database may include the first and last names of children, login details for cloud accounts, the email addresses, telephone numbers and the birthdates, photographs and text messages of children and it may also include GPS details for the child. In short I understand that it contains enough information to allow a predator to know the exact whereabouts of children (ie: track the child's mobile telephone) and even contact the child on its mobile telephone.

27. It has been reported by uKnowKids that a security researcher has allegedly taken advantage of a security flaw in the uKnowKids platform and has obtained unauthorised access to the uKnowKids database.[2] It is also reported that the security researcher has allegedly stated that it "is the right of any member of the public accessing information that is configured for public access and being offered to the public".[3] Whilst it is also reported that the researcher did not have bad intentions and is a *white hat*, the example highlights just how serious unauthorised access to data can be, the importance of immediate notification and the level and detail of information held by entities.

28. uKnowKids made a detailed notification of the alleged breach within a week of becoming aware of the access and that notification was made to the general public, to its customers and to US authorities. The notification included information on the nature of the breach and what steps had been taken to contain the breach and an indication that it would keep customers informed of the matter. That notification can be found at: http://resources.uknowkids.com/blog/breaking-news...-a-uknow-database-was-breached-by-a-hacker-and-here-are-the-facts-as-we-know-them-right-now. It was to notify individual customers if that customers data was part of the data taken. That notification would have

[1] www.uknowkids.com.
[2] http://resources.uknowkids.com/blog/breaking-news...-a-uknow-database-was-breached-by-a-hacker-and-here-are-the-facts-as-we-know-them-right-now.
[3] http://www.csoonline.com/article/3036556/security/uknowkids-com-responds-to-data-breach-says-proprietary-ip-also-exposed.html?utm_content=buffer7003c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

allowed affected individuals to immediately take steps to protect the child and the information.

29. Within the Australian context there is no current requirement, under the *Privacy Act* only,[4] for a similar notification to be made by an AAP entity.

30. However, even with the proposed amendments in force, parents would not be able to immediately protect their children due to the possible delay in notification of any breaches. Indeed, if you assume that uKnowKids was an APP entity and the privacy amendments proposed by the Bill were in force then uKnowKids would not have to, (if only the *Privacy Act* applied), notify individuals or the Commissioner of the breach until it had completed its assessment of a breach and that could take up to a period of 30 days. In the present case uKnowKids had the presence of mind to make a notification quickly but other service providers may not. If similar material had been taken by a bad actor rather than a person merely wishing to highlight the security flaw, then in that 30 day period the bad actor could have passed details of vulnerable children to networks of individuals around the world and neither the parents of those children nor the children themselves, would not have known to be especially vigilant as to safety nor would they have known to take mitigating steps such as changing the telephone number of the children or resetting cloud passwords to avoid the child being tracked.

[4] Other obligations aside.