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)*	Australian Communications Consumer Action Network (ACCAN)
Contact details *(one or all of the following: postal address, email address or phone number)*	Jeremy Riddle [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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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 on Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

Submission by the Australian Communications Consumer Action Network to the Australian Attorney-General's Department

4 March 2016

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

Jeremy Riddle
Policy Officer

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

1. Introduction

ACCAN thanks the Attorney General's Department for the opportunity to provide feedback on the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill) and its associated supporting documents.[1]

ACCAN would like to commend the Attorney General's Department for taking such a strong and positive stance in its Regulatory Impact Statement on the introduction of a mandatory scheme. A mandatory scheme is in the best interests of Australian consumers affected by serious data breaches as it allows them to take action to mitigate potential harms such as identify theft and financial loss. It gives consumers confidence that in the event of a breach they will be able to manage their own personal information.

ACCAN broadly supports the introduction of a mandatory notification scheme for serious data breaches, as described in Option Two of the Regulation Impact Statement and as set out in the Exposure Draft. We do, however, have a limited number of recommendations that we believe will improve outcomes for consumers.

1.1. Summary

ACCAN recommends that the Bill be amended as set out in this submission. Our key recommendations are summarised as follows:

1. That the *'Relevant matters'* in determining whether there is a real risk of serious harm in section 26WB(3) are revised; namely that section 26WB(3)(i) is either removed or reworded for reasons given in 1.2.1.

2. That the definition of *'as soon as practicable'* in section 26WC(2) is reviewed and the timeframe for carrying out a reasonable assessment is shortened for the reasons given in 1.2.2.

3. That the exception in section 26WC(6)-(10) '*Commissioner's notice*' is revised to include maximum timeframes for entities applying for an exception and for the Commissioner's response to applications for reasons given in 1.2.3.

This submission also discusses potential measures to deter future serious data breaches, including:

- that the Commissioner should require undertakings from breached entities that will be enforceable in the Federal Court should the breach reoccur; and

- that all serious data breaches, their consequences, and details of the way in which they were handled are published in an Annual Report.

[1] Discussion Paper, Regulatory Impact Statement, and Explanatory Memorandum.

1.2. Recommendations

1.2.1. Section 26WB(3)(i) should be revised or removed from the Bill

Proposed section 26WB(3) sets out the relevant matters to be taken into account in determining whether there is a real risk of serious harm to an individual, and therefore whether a serious data breach has taken place. Subsection (i) states that a relevant matter is "if the entity has taken, is taking, or will take, steps to mitigate the harm…".

As the Bill is currently drafted, entities could avoid the requirement to notify affected individuals by reacting quickly to resolve or mitigate any potential harm to a level where it is no longer considered 'serious'.

ACCAN believes that whether a serious data breach has occurred and should therefore be notified to individuals should not be negated after the fact by an entity's actions, no matter how well-intentioned or effective. Whether there is a 'real risk of serious harm' and therefore a 'serious data breach' should only be assessed as at the time of the breach.

Consumers have an interest in knowing that a serious breach has occurred as soon as possible. The knowledge of a breach may affect their decisions on whether or not they want to keep receiving services from an entity. Consumers also have an interest in being notified as soon as possible after a serious data breach so that they have the opportunity to take their own mitigating steps.

However, if section 26WB(3)(i) is to remain where it is, ACCAN is of the view that the words "or will take" are unnecessary and should be removed. The current wording opens the gate for entities to argue that the breach is not serious and does not require notification due to mitigating steps they plan to take in the future. However there is no guarantee that the entity will take such action, or of how successful it will be in mitigating potential harms.

1.2.2. The timeframe for carrying out a reasonable assessment under section 26WC should be reduced

Section 26WC(1) sets out the steps an entity must take if it is (or ought to be) aware that there are reasonable grounds to believe that there has been a serious data breach. These steps are to be taken "as soon as practicable after the entity becomes so aware…".

Section 26WC(2) explains that for the purposes of 26WC(1):

> "***…as soon as practicable*** includes time taken by the entity in carrying out a reasonable assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to a serious data breach of the entity, so long as that assessment is carried out within 30 days…"

A 30 day period to carry out such an assessment is too long and should be revised. This is particularly important as breaches of personal information could be a matter of life and death for affected individuals. Take as one example victims of domestic abuse whose whereabouts or contact details become known to abusive partners.

The proposed 30 day timeframe does not strike an appropriate balance between the risk of real and serious harm to affected individuals and the needs and capabilities of entities. It is in the best interest of consumers for entities to undertake such assessments in as little time as is possible.

1.2.3. The Commissioner's notice exception in section 26WC(6)-(10) should include maximum timeframes

The Commissioner's notice exception allows the Commissioner to exempt an entity from its obligation to notify individuals of a serious data breach if he or she is satisfied that it is in the public interest to do so (section 26WC(7)).

ACCAN submits that there should be maximum timeframes imposed for:

a) an entity to submit an application for an exemption; and
b) the Commissioner to either refuse the application or grant the exemption

so that individuals affected by a serious data breach are not left without notification for unnecessarily long periods of time. The longer the exemption process takes, the higher the risk is that individuals will suffer real and serious harm as a result of the data breach.

1.3. ACCAN has suggested measures to deter future serious data breaches

1.3.1. Require undertakings enforceable in the Federal Court

Entities that are required to notify of serious data breaches under a mandatory scheme should be required to provide an undertaking to the Commissioner. The undertakings will be enforceable in the Federal Court and will therefore act as a deterrent against foreseeable future breaches.

1.3.2. Publish an Annual Report of serious data breaches

Legislation should require the publication of an Annual Report of all serious data breaches. The report would include details of the breach, the consequences of the breach, and the actions that were taken to mitigate and rectify any harm caused. Such a report would increase the transparency of the mandatory scheme, and naming the entities responsible for serious data breaches would decrease the risk of breaches occurring in the future.

1.4. Additional comments

ACCAN would like to acknowledge that although it supports the scheme set out in the Bill as an important consumer protection, its application would still be limited to entities regulated by the Privacy Act 1988 (the Act). As stated on page 23 of the Regulatory Impact Statement, in 2013 about 94% of entities on the Australian Bureau of Statistics' Business Register were below the $3 million annual turnover threshold, and therefore were unlikely to be governed by the Act. Under the proposed Bill, a small business that collects personal information and does not meet the threshold could suffer a massive and harmful breach, but would not have to notify affected individuals. ACCAN believes the limited application of the Act is something policymakers should consider in any future review of privacy legislation.