Australian Government
Australian Law Reform Commission

Professor Rosalind Croucher AM
President

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

Sent via privacy.consultation@ag.gov.au

11 February 2016

Dear Sir/Madam,

ALRC Submission: Exposure draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

I refer to the invitation for submissions on the exposure draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill).

The Bill would amend the *Privacy Act 1988* (Cth) to insert a new pt IIIC, which would define when a 'serious data breach' occurs and explain when and in what form notification of serious data breaches is required.

The Discussion Paper published with the Bill observes that the Bill is based on the recommendation made in the ALRC's 2008 Report, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108). Recommendation 51–1 of that Report stated:

> The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:
>
> (a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
>
> (b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number.
>
> (c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:
>
> (i) whether the personal information was encrypted adequately; and
>
> (ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the *Privacy Act* (provided that the personal information is not used or subject to further unauthorised disclosure).
>
> (d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.
>
> (e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

Australian Law Reform Commission
Level 40, MLC Centre
19 Martin Place
Sydney NSW 2000

Postal Address
GPO Box 3708
Sydney NSW 2001

Tel (02) 8238 6333
Fax (02) 8238 6363

Web www.alrc.gov.au
Email info@alrc.gov.au

More recently, the ALRC considered legal liability for data breach in its inquiry into remedies for serious invasions of privacy. The 2014 Report, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123), concluded that, in general, regulatory responses (including mandatory data breach notification) are a better way to deal with data breaches than a civil action for invasion of privacy: see ALRC 123, para 7.62.

The Bill would implement the 2008 ALRC recommendation by requiring agencies and organisations regulated by the *Privacy Act* to provide notice to the Australian Information Commissioner and affected individuals of a serious data breach. The Bill provides that a data breach is a serious data breach where there is a 'real risk of serious harm to the individual' to whom the information relates as a result of the data breach (the affected individual)—based on the standard recommended by the ALRC.

In addition, the Bill provides for regulations to specify particular situations that may also be serious data breaches, even if they do not necessarily reach the threshold of a real risk of serious harm. The Explanatory Memorandum accompanying the Bill notes that 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—an approach that is also consistent with the ALRC recommendation.

The exposure draft Bill provides for exceptions to the notification requirement, including that law enforcement bodies will not be required to notify affected individuals if notification would be likely to prejudice law enforcement activities: see Bill, cl 26WC(5).

The ALRC recommended that the Privacy Commissioner (as the recommendation was made before the establishment of the Office of the Australian Information Commissioner) should have a broad discretion to waive the notification requirement where the Commissioner does not consider that it would be in the public interest to notify. This would include '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': see ALRC 108, para 51.94. However, the ALRC did not otherwise consider the desirability of a more general exception to the notification requirements, or the scope of any such exceptions.

Subject to this reservation, the ALRC considers that the Bill is consistent with the approach to data breach notification recommended by it in 2008 and welcomes this legislative initiative.

Thank you for this opportunity to comment on the exposure draft Bill. If you require any further information please do not hesitate to contact me on [redacted].

Yours sincerely,

[redacted]

Professor Rosalind Croucher AM