



Australian Government

Australian Law Reform Commission

Professor Rosalind Croucher
President

Mr Tim Bryant
Inquiry Secretary
Senate Legal and Constitutional Affairs Committee
Parliament House
Canberra ACT 2600

20 June 2013

Dear Mr Bryant

Inquiry into the Privacy Amendment (Privacy Alerts) Bill 2013

The Australian Law Reform Commission welcomes the release of the Privacy Amendment (Privacy Alerts) Bill 2013.

The Bill implements a recommendation in Chapter 51 of the ALRC report, *For Your Information—Australian Privacy Laws and Practice*, Report 108 (May 2008). The recommendation is attached to this submission, for your convenience, and it is discussed at some length in the Bill's Explanatory Memorandum.

The rationale for our recommendation is set out on pages 1687-96 of volume 2 of the ALRC's report, and includes the following:

51.73 The *Privacy Act* should provide for notification by agencies and organisations to individuals affected by a data breach. This requirement is consistent with the Privacy Act's objective to protect the personal information of individuals. 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.

...

51.76 Notification requirements are ... not reliant on establishing that an agency or organisation has not complied with its data security obligations. Nor are the provisions aimed at 'punishing' bodies when a breach occurs. Rather, the primary rationale for data breach notification laws is that notifying people that their personal information has been breached can help to minimise the damage caused by the breach. Notification acknowledges the fact that a data breach potentially can expose an individual to a serious risk of harm. By arming individuals with the necessary information, they have the opportunity, for example, 'to monitor their accounts, take preventative measures such as new accounts, and be ready to correct any damage done'.

...

51.79 The legal requirement to notify in the case of serious breaches is necessary because, as explained above, there is a risk that the uncontrolled market may 'undersupply

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

Postal Address:
GPO Box 3708
Sydney NSW 2001

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

Web www.alrc.gov.au
Email rosalind.croucher@alrc.gov.au

notification'. That is, because of the reputational damage to organisations that notification can cause, organisations may not have sufficient incentives to notify customers voluntarily of a data breach.

51.80 A data breach notification requirement also can provide incentives to improve data security. The reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives to improve security.

51.81 Notification also plays an important role in keeping the market informed of the privacy practices of organisations. As Professor Robert Baldwin and Professor Martin Cave suggest, 'competitive markets can only function properly if consumers are sufficiently well informed to evaluate competing products'. In the absence of notification, a data breach causes an 'information inadequacy', as the organisation knows that there has been an unauthorised acquisition of an individual's personal information, but the individual affected does not. Until the individual is notified of a data breach, therefore, there may be inadequate information in the market for individuals to evaluate the different information-handling practices of organisations.

A copy of the report is available on the ALRC's website at www.alrc.gov.au, if further background information would be of interest to the Committee.

Sincerely,

Professor Rosalind Croucher