



Law Council  
OF AUSTRALIA

Professor (Emeritus) Sally Walker  
Secretary-General

29 November 2012

Mr Richard Glenn  
Assistant Secretary  
Business and Information Law Branch  
Attorney-General's Department  
4 National Circuit  
BARTON ACT 2600

Via email: [privacy.consultation@ag.gov.au](mailto:privacy.consultation@ag.gov.au)

Dear Mr Glenn

### **Discussion Paper: Australian Privacy Breach Notification**

The Privacy Committee of the Business Law Section of the Law Council of Australia (the Committee) is pleased to provide this submission in response to the Attorney-General's Department Discussion Paper on Australian Privacy Breach Notification.

The Committee recognises that the escalating quantity and sensitivity of data collected and retained by organisations, combined with increasingly sophisticated IT systems and technologies, means that the issue of mandatory data breach notification is a topical and relevant one.

While the Law Council previously supported, in principle, a mandatory data breach notification it now believes it is premature to make any expansive submissions on the necessity for, and appropriate provisions to be contained in, any mandatory data breach notification laws. The introduction of the amendments to the *Privacy Act* contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* is likely to bring about a different privacy landscape and we suggest that the effectiveness and consequences (both intended and unintended) of those amendments should be experienced and properly considered before further amendments are made.

The Amending Act proposes more rigorous protection of personal information including significant pecuniary penalties for serious or repeated interference with the privacy of an individual. The Committee suggests that this in itself may be sufficient to achieve greater compliance by organisations.

Further, the Amending Act proposes to expand the functions and powers of the Privacy Commissioner, including increasing the Commissioner's ability to resolve complaints, conduct investigations and promote compliance with privacy obligations. The Committee submits that such changes may sufficiently address the same issues that any mandatory data breach notification legislation would seek to resolve. In any event, it would be

GPO Box 1989, Canberra  
ACT 2601, DX 5719 Canberra  
19 Torrens St Braddon ACT 2612

Telephone +61 2 6246 3788  
Facsimile +61 2 6248 0639

Law Council of Australia Limited  
ABN 85 005 260 622  
[www.lawcouncil.asn.au](http://www.lawcouncil.asn.au)

appropriate to wait and see how the new provisions work in practice before adding another layer of legislation.

The Committee submits that already-stretched resources at the Office of the Australian Information Commissioner will be substantially affected by the expansion of the functions and powers of the Commissioner proposed under the Amending Act. Any mandatory data breach notification scheme should therefore be considered in the context of the available resources at the OAIC and any subsequent limitations in its governance and policing of privacy obligations of organisations and agencies. If too great a burden is placed on the OAIC, it may be unable to effectively perform the functions conferred upon it by the *Privacy Act 1988 (Cth)* and other laws.

Until such time as any new privacy legislation has been passed by the Parliament and its effectiveness analysed, the Committee is of the view that the existing data breach notification regime, particularly the voluntary data breach notification guidelines issued by the Office of the Australian Information Commissioner, is appropriate. The Committee submits that reputational consequences alone currently provide a good incentive for organisations to implement high security standards and to voluntarily notify the OAIC in circumstances where it is appropriate to do so.

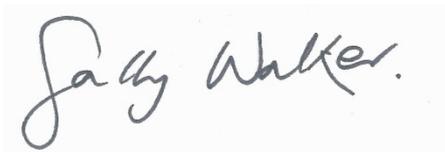
If the Government were to proceed to introduce mandatory data breach reporting, the Committee submits that the legislation would need to define a 'data breach' in clear and objective terms. A regime requiring reporting of *all* privacy breaches in all circumstances would be unnecessary and place unacceptable strain on business and the OAIC. Rather, the Committee supports the test propounded by the ALRC in its 2008 report and that adopted in the OAIC guide, namely, that a data breach should be reported only where there is a *'real risk of serious harm'* to an individual or group of individuals.

The Committee may wish to provide further comment if there is an opportunity to do so at any subsequent stage.

Please note that, due to time constraints, this submission has not been considered by the Directors of the Law Council of Australia.

If you have any questions regarding this submission, in the first instance please contact the Committee Chairman, Olga Ganopolsky, on 02-9278 7837 or via email: [olga.ganopolsky@veda.com.au](mailto:olga.ganopolsky@veda.com.au)

Yours sincerely

A handwritten signature in black ink that reads "Sally Walker". The signature is written in a cursive, flowing style.

**Professor Sally Walker**  
**Secretary-General**