THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: BusLaw: GUlb1096098

4 March 2016

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

By email: privacy.consultation@ag.gov.au

Dear Sir/Madam,

Exposure draft - Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

The Law Society of NSW appreciates the opportunity to comment on the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 ("Bill") and accompanying Mandatory Data Breach Notification Discussion Paper.

1. Overview

The Bill will implement new obligations affecting almost all corporations (over a certain size) and Commonwealth agencies in Australia. The Law Society suggests that, to minimise the regulatory burden, adequate time should be allowed for implementation, after finalisation of the text of the legislation, and promulgation of the regulations. Most importantly, the scope of the obligations must be sufficiently clear, so as not to impose an unreasonable burden on Australian businesses.

The Law Society notes that, importantly, the Bill provides a mechanism for individuals whose personal information has been compromised in a serious data breach, to take remedial steps to avoid potential adverse consequences.

The Bill should effectively balance the interests of businesses with those of affected customers. In doing so, legislators must take into account the detrimental effect that notification obligations can have on the image, brand and profits of a business.

2. Scope of obligation

Under section 26WC, entities must notify affected individuals and the Australian Information Commissioner ("AIC") if a 'serious data breach' has occurred. Section 26WB provides that a 'serious data breach' occurs when there is unauthorised access or disclosure of specific information held by specified entities, which results in a 'real risk of serious harm'.

Section 26WG attempts to define the existence of 'real risk', stating that the risk must not be 'remote'. Although this provides some assistance, it does not go far enough to delineate the scope of the obligation. In addition, no attempt is made to define the term 'serious', although the explanatory memorandum at [129] indicates that the intention is that it means 'not minor'.

Serious consideration should be given to streamlining the description of data breach related risks and their likely impacts. If a clear threshold is not established, businesses may feel obliged to notify individuals and the AIC in a wide range of scenarios, as a precaution to avoid the risk of breaching their obligations under the proposed legislation. This could lead to 'notification fatigue', a rise in compliance costs and an unanticipated increase in the administrative burden to be borne by businesses.

3. Interaction of sections 26WB(1) and 26WC

Section 26WB(1) states that, for an Australian Privacy Principles ("APP") entity that holds personal information and is required to comply with the APPs, the 'serious data breach' definitions apply. Section 26WC then provides 'if an entity is aware' (of a serious data breach) then it must notify by following the procedural requirements in section 26WC. This suggests that all entities, whether or not they are an entity that falls under section 26WB(1), need to notify. It can also be read that if the serious data breach concept does not apply, section 26WC is not triggered (therefore there is no need to notify). That is, section 26WB must be satisfied first before s26WC is triggered.

The drafting of these two sections should be amended to clarify how these two sections interact with each other.

4. Application of the State government contract exemption under the *Privacy Act 1988*

Businesses that have obligations under State government contracts need clarity as to whether serious data breaches in relation to personal information that falls under the State government contract exemption (section 7B(5)) needs to be reported. It is not clear whether, because an act or practice falls under the exemption, any serious data breach that arises from those acts or practices is also exempt from the notification requirement. The current drafting of sections 26WB and 26WC requires amendment to clarify how those sections interact when read together with section 7B(5).

If you have any questions in relation to this submission, please contact Liza Booth, Principal Policy Lawyer, by email at liza.booth@lawsociety.com.au or phone (02) 9266 0202.

Yours faithfully,

Gary Ulman
President