AmCham

Friday, 4 March 2016

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

***Also by Email:*** privacy.consultation@ag.gov.au

**Proposed Mandatory Data Breach Notification Scheme**

Dear Sir/Madam,

The American Chamber of Commerce in Australia is writing in response to the request for submissions as set out in the Consultation paper "Mandatory Data Breach Notification" issued by the Attorney-General's Department in December 2015.

The American Chamber of Commerce in Australia - better known as AmCham - was founded in 1961 by Australian and American businesses to encourage the two-way flow of trade and investment between Australia and the United States, and to assist its members in furthering business contacts with other nations. In pursuing this goal, AmCham has grown and diversified. It finds itself not only representing the United States' business view, but also speaking increasingly for a broad range of members involved in the Australian business community.

AmCham represents the interests of American companies undertaking business activity in Australia. American investment accounts for 24 per cent of all foreign investment in Australia which makes it, by far, the single largest foreign investor in Australia. We also have significant membership by Australian companies and endeavour to represent their interests equally.

***Privacy Amendment (Notification of Serious Data Breaches) Bill 2015***

The Australian Government has made a commitment to introduce a Mandatory Data Breach Notification scheme (the 'Scheme') that protects individual privacy without placing an unreasonable regulatory burden on business.

The American Chamber of
Commerce in Australia

Suite 9, Ground Level
88 Cumberland Street
Sydney NSW 2000

Tel: +61 2 8031 9000
Email: nsw@amcham.com.au
Web: www.amcham.com.au

The proposed scheme applies to entities regulated by the Privacy Act 1988 (the 'Act') operating in Australia. Under the scheme such entities are required to notify the Australia Information Commissioner (the 'Commissioner') in the Office of the Australian Information Commission (OAIC) and affected individuals of serious data breaches as soon as practicable after the entity is aware, or ought to have been aware, that there are reasonable grounds to believe that there has been a serious data breach.

Under the scheme, a serious data breach is deemed to occur if there is unauthorized access to, or unauthorized disclosure or loss of, personal information that creates a *real risk of serious harm* to any of the individuals to whom the information relates.

The notification must include the identify and contact details of the entity, a description of the serious data breach, the kinds of information concerned, and recommendations about the steps that individuals should take in response to the serious data breach. When notifying those affected, the entity may use the method of communication, normally used to communicate with that individual. Failure to comply may result in an investigation and enforcement action by the Commissioner.

***Breaches Suffered by Vendors and Service Providers***

Pursuant to the proposed scheme, if a service provider holds personal information on behalf of a company, and the service provider suffers a breach, it appears that the service provider will have primary responsibility for the breach. This raises a couple of practical and legal issues.

Firstly, if the service provider is a small business, it may be exempt from complying with the Act and may therefore be outside the requirements of the data breach reporting provisions. This suggests that large companies could lodge their data in small independent Australian service provider companies in order to take advantage of this apparent loophole.

Secondly, the intention of the scheme is to impose a notification on each entity that holds the personal information that is affected by the data breach. In this scenario, the notification obligation would be on the service provider. But that raises a practical issue, in that the existence of the service provider may be unknown by the affected individuals (typically customers) because the individuals have a commercial relationship with the principal company (eg. a retailer). In practice, the retailer would probably want to send the notice itself, or at least control the content and manner of the notice if it was given by the service provider.

Further, if the retailer gives a breach notice to its customers, the service provider has not itself complied with its obligation to give a breach notice. This leaves open the question of whether a notice by the retailer is sufficient to fulfil the obligations of a service provider, even though the notice is sent to the same individuals in respect of the same data breach.

Interestingly, the position is clearer if the service provider is located overseas and if Australian Privacy Principal 8.1 applies to the circumstances (which is likely to be true in

most cases). In this case, the Australian entity will usually be deemed to be the holder of the information and, by inference, to have suffered the data breach.

*Notification of Individuals Outside of Australia*

The proposed scheme refers to individuals only and fails to differentiate between individuals inside and outside Australia. While this is probably as it should be, otherwise greater protection would be afforded to the personal information of Australians over foreign citizens, this broad application raises additional practical complications.

Firstly, an Australian company would be required to notify overseas individuals even though the domestic laws of those individuals do not require notification.

Secondly, the Australian company could hold information on behalf of its overseas related companies. In practice, this could mean that "Retailer Australia" may be required to give breach notices to the customers of "Retailer USA". As noted above, Retailer USA would probably want to give the breach notice directly in order to better preserve its customer relationships. However, once again, it is not clear whether that would fulfil the obligations of Retailer Australia.

While AmCham recognises the importance of protecting individual privacy and the need to provide individuals an opportunity to take remedial steps to avoid / mitigate adverse consequences as a result of a data breach, we urge the Attorney-General's Department to consider the practical implications of the proposed scheme, which in its current form, may place unreasonable regulatory burdens on business should an entity, with no prior relationship with the affected individuals, not be in a position to delegate its obligations to an entity with the commercial relationship.

In closing, AmCham recognizes that the Scheme has many other aspects and implications beyond the specific retail and logistics considerations raised in this brief submission. AmCham deliberately has limited our submission to raise only those concerns expressed by our membership about these particular aspects of the Scheme. This limited submission therefore should not be construed as conferring approval on or agreement with other aspects of the Scheme about which we may not have commented.

Yours sincerely,

[redacted]

Niels Marquardt
U.S Ambassador (ret.),
Chief Executive Officer