Microsoft Australia

Submission to the Serious Data Breach Notification Consultation

March 2016

Your details

Name/organisation *Microsoft Pty Ltd* *David Masters* *Corporate Affairs Manager*	
Contact details [contact details redacted]	

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.
  Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? YES / **NO**

Response to the Serious Data Breach Notification Consultation

Microsoft is pleased to respond to the Attorney-General's Department's (**AGD**) request for submissions featured in the Discussion Paper in relation to the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (**Bill**), Explanatory Memorandum and the accompanying Early Assessment Regulatory Impact Statement.

Microsoft is supportive of the new Bill and its intention '*to improve the privacy of Australians without placing an unreasonable regulatory burden on business',* and encourages the introduction of the Bill into Parliament in 2016.

We believe the Bill strikes an appropriate balance between protecting the privacy of individuals, without imposing an overly administrative burden on Australian Privacy Principal Entities.

Microsoft looks forward to guidance from the Office of Australian Information Commissioner (OAIC) on the Bill. We encourage the AGD to continue to work in close consultation with industry with regards to both the development of future guidance and regulations, and we welcome any opportunity to be engaged.

We also encourage the AGD to provide further clarifications and guidelines on the types of incidents that trigger notification obligations, with a view to avoid over-reporting that may occur when organisations are unsure of what constitutes a serious data breach, as well as the notification fatigue and administrative burden that would accompany it.

Microsoft's approach to privacy

Protecting and maintaining customer privacy is an utmost priority for Microsoft. We understand that data breaches put consumers at risk of fraud and identity theft, and jeopardise the trust relationship between consumers and business. One of the ways organisations can give customers confidence that their data will be handled appropriately is to ensure that in the event there is a serious security breach that gives rise to a real risk of serious harm, they will be notified as soon as practicable.

For almost 20 years, Microsoft has been a leader in developing industry leading privacy policies, compliance programs and security measures that we apply across our online and cloud services. Our commitment to the privacy of our customer data is backed by the Microsoft Online Services Privacy Statement, which describes the specific privacy policy and practices covering customer data in the Microsoft Cloud.

Today, Microsoft's services are used by over a billion customers around the globe. Microsoft understands that data protection and privacy is a truly international issue. Microsoft adheres to existing standards and regulations internationally, and seeks to anticipate and comply with any developments as they arise. We were the first major cloud provider to adopt the first international code of practice for cloud privacy, ISO/IEC 27018. This standard requires that providers comply with legislative requirements to disclose privacy breaches where they exist.

Further, the passing of this legislation could see Australia rise on the BSA Global Cloud Computing Scorecard from its already high ranking of 2 out of 24 countries. The only negative Australia received on the 66 agenda checklist of cloud readiness was in not having a breach notification law.

Therefore, we welcome the alignment of Australian privacy standards with those that exist internationally as a means to achieve consistency and avoid uncertainty, and provide the opportunity for Australia to maintain its reputation as a leader in privacy protection globally.

The Bill

In 2013, Microsoft welcomed the initial draft data notification bill. As such, we are also supportive of the 2015 bill and the majority of changes and additions that accompany it.

Microsoft agrees that a serious data breach occurs in instances of unauthorised access, disclosure of loss of personal information (or certain other information) held by an entity, with the condition of a real risk of serious harm.

We look forward to further consultation on the information prescribed by regulations that will be automatically considered to be a serious data breach upon unauthorised access, disclosure or loss, without the need for an assessment of harm.

We note from the Regulation Impact Statement that it would be possible to prescribe specific information such as 'specific government identifies'. We also understand that the Commissioner is planning to issue guidance material to help entities assess whether a 'serious data breach' has occurred, and how to comply. We look forward to consulting with the Commission on this guidance, to provide further clarification to entities undertaking breach analysis.

We agree that serious harm, in this context, should include physical, psychological, emotional, economic and financial harm, as well as harm to reputation. We also agree with the factors to be taken into account when determining whether a risk of serious harm existed.

Further, the addition of the 30-day period within which time an organisation can make an assessment of whether there are reasonable grounds that a serious data breach has occurred, will helpfully account for times where an initial cause for concern reveals that there is no reasonable risk of a serious data breach.

However, we do hold some reservations on the operation of the proposed section 26WC(1) which requires the entity to which the serious data breach has occurred, to issue the notices. Given the increasing use of cloud services which provide processing, storage, database and other services, it is increasingly likely that a cloud service provider (or contractor) does not have the ability to communicate with the individual data subjects, where the entity who collected the data stored (primary) in that service likely does.

In fact, for privacy reasons, many cloud contracts (including Microsoft's) specifically limit the ability of the cloud service provider to access customer data; and therefore also limit the ability of the provider to make an accurate determination of whether or not serious harm has occurred.

Placing the primary responsibility for notifying affected individuals of serious data breaches on the entity who owns the customer relationship and was responsible for the date collection, is consistent with how the Office of the Australian Information Commissioner ("OAIC") considers APP entities (as defined in the *Privacy Act 1988).* In this, the APP entity is responsible for any mishandling of information and the consequent breach of the APPs, even though the mishandling may have occurred while the information was in the contractor's physical possession

We also refer to the OAIC's own guidance on the new Australian Privacy Principles, specifically APP 8, which distinguishes between use and disclosure for the purposes of determining whether an offshore disclosure has been triggered by the use of cloud services.

We feel that this use vs disclosure is a sensible distinction that should carry over to considerations of a breach notification. To borrow from this guidance, we feel that if the contractor is contracted "*for the limited purpose of performing the services of storing and ensuring the entity may access the personal information*"[1] and the contract clearly stipulates this arrangement, then the onus on the contractor should be to notify the collection or primary entity of a potential breach; and that they should then determine whether serious harm has occurred and communicate with the affected individuals.

While we believe that 26WC (1)(d) may allow for an alternative form of notification in this circumstance, we feel that the bill and the associated guidance should specifically address this increasingly common, primary entity-contractor scenario.

Next Steps

Microsoft appreciates the opportunity to comment and supports the introduction of the Bill into Parliament in 2016. We do not anticipate any significant administrative or compliance burdens from its introduction as we have well established systems for data breach notification within our online services.

As flagged within this submission, Microsoft would appreciate the opportunity to contribute to any future consultation in the development of future regulations or guidelines.

[1] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.