Microsoft Submission to the Queensland Department of Justice and Attorney-General Review of the *Information Privacy Act 2009:* Privacy Provisions

General Comments

Microsoft Australia welcomes the opportunity to comment on the Queensland Government's review of the *Information Privacy Act 2009: Privacy Provisions*.

As a general principle, Microsoft strongly believe in being open and transparent with our customers, including Government, on privacy and data use.

In line with this commitment on transparency and privacy, we have developed online Trust Centres that provide additional information on privacy, security and data issues for all of our cloud services including: Office 365, Dynamics CRM Online, and Windows Azure.

At a broad level we are extremely comfortable with the Privacy regime operating across Queensland Government and we have worked very constructively with our Queensland Government clients to ensure that they meet their requirements under the legislation.

Our major comments are related to improving the consistency of the *Information Privacy Act 2009* with the incoming amendments made to the Federal *Privacy Act 1988*, through the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and the privacy regimes operating in other jurisdictions in Australia; rather than the substance of the legislation.

Responses to Questions

Question 1.0: What would be the advantages and disadvantages of aligning the IPPs with the APPs, or adopting the APPs in Queensland?

Consistency is a good thing for business, and we support standardisation of privacy regimes across all Australian jurisdictions.

Better alignment between the IPPs and APPs (or even adoption of the APPs under the *Information Privacy Act 2009)* will enable organisations operating in Queensland to develop privacy policies and procedures; and privacy protecting terms and conditions within contracts that can clearly be shown to support both private sector and public sector clients in Queensland.

We do not believe that there are any disadvantages associated with standardising Queensland's privacy principles with those that are in force in other Australian jurisdictions.

Question 5.0: Should section 33 be revised to ensure it accommodates the realities of working with personal information in the online environment?

Question 6.0 Does section 33 present problems for agencies in placing personal information online?

Question 7.0 Should an 'accountability' approach be considered for Queensland?

Section 33 of the Act should be amended to be consistent with other jurisdictions.

It currently sets a much higher bar to the transfer of personal information outside of Australia then is the case elsewhere.

As a suggestion, APP 8 under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which regulates the circumstances in which Australian entities can send information offshore, provides useful guidance on the requirements that must be met when data is sent overseas as part of a services agreement. In our view APP 8 strikes an appropriate between the rights and interests of information subjects, on the one hand, and information collectors, on the other. APP 8 gives information collectors the flexibility to determine what steps are reasonable in a particular set of circumstances, and in our experience collectors discharge this obligation via a combination of due diligence, contractual commitments, and independent certification and verification. By contrast, section 33 is inflexible and prescriptive, which particularly creates issues in the fast changing environment of the technology sector.

We also support the further draft guidance from the Office of the Australian Information Commission (OAIC) that APP 8 only applies if personal information is "disclosed" to an overseas recipient; and that the provision of a standard service that stores and manages personal information (as in a cloud service) constitutes a 'use' and not a 'disclosure'.

The recent draft guidance provided by the OAIC on the use of overseas contractors or offshore hosted cloud services is copied below:

8.12. *However, in limited circumstances, providing personal information to an overseas contractor to perform services on behalf of an APP entity may be a 'use' [ie not a "disclosure"]. In these circumstances, the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of storing and managing personal information, and:*

- *the contract between the entity and the overseas cloud service provider binds the provider not to use or disclose the personal information except for the limited purpose of storing and managing the information*
- *the contract requires any sub-contractors to agree to the same obligations, and*
- *the contract between the entity and the cloud service provider gives the entity effective control of the information. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able access the information and for what purposes, and what type of security measures will be used for the storage and management of the personal information.*[1]

In our submission to the Office of the Australian Information Commissioner, we have suggested some strengthening of this guidance in order to ensure that appropriate protections are imposed in an offshoring context; and that it is clear that a disclosure is triggered if the information is used for datamining, advertising or marketing purposes.

In addition, Section 35 provides that "*An agency entering into a service arrangement must take all reasonable steps to ensure that the contracted service provider is required to comply with part 1 or 2 and part 3, **as if it were the agency**, in relation to the discharge of its obligations under the arrangement".* Specifically in relation to public cloud services provided by a contracted service

[1] *Chapter 8 – APP 8 – cross-border disclosure of personal information Draft Version, September 2013,* Office of the Australian Information Commissioner, viewed at: http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_8.pdf

provider, it is impractical to mandate that an Agency require that provider to comply with all of those specific parts, *as if it were the agency*.

Specifically in relation to the IPPs, since the contracted service provider is not the collector of the personal information, has no relationship with the end user and does not know where personal information may exist within data hosted for an Agency on the service, a contracted service provider is not in a position to comply with some IPPs. For example, IPP 2 and 3 which relate to an Agency's obligations on collection of personal information cannot be complied with by a public cloud service provider since it does not collect personal information from end users and so cannot explain to them the purpose of collection.

IPP 5 obliges an Agency to take reasonable steps to ensure that a person can find out what personal information an Agency holds about them. IPP 6 obliges the Agency to give that person access to that personal information. IPP 7 requires an Agency to take reasonable steps (including by making amendments) to ensure the personal information is accurate, relevant and complete. A public cloud service provider cannot comply with any of these IPPs since such providers do not know what, if any personal information an Agency may hold about an end user nor where such information may exist within the data hosted by them on behalf of an Agency.

The Agency knows what personal information it has collected about an individual, where such information may exist within data hosted by such providers and the Agency has continuous access to such information. For these reasons the Agency is the only party that can comply with these kinds of obligations in so far as they apply to personal information hosted in a public cloud. Apart from ensuring that the public cloud service provider takes reasonable steps to protect personal information from loss, misuse or unauthorised disclosure and undertakes not to use such information for any purpose other than to provide the service, there is no need to make a public cloud service provider comply with these other obligations *as if it were the Agency*.

14.0 Should IPP 4 be amended to provide, in line with other IPPs, that an agency must take reasonable steps to ensure information is protected against loss and misuse?

To improve the consistency of IPP 4 with other Australian privacy regimes (including the new APPs), we recommend that IPP 4 be amended from "must ensure" protection against loss and misuse to "must take reasonable steps".

15.0 Should the words 'ask for' be replaced with 'collect' for the purposes of IPPs 2 and 3?

We support the proposed amendment of the words 'ask for' to be replaced with the word 'collect' in IPPs 2 and 3 to ensure consistency with other Australian jurisdictions.