SUBMISSION

SENATE FINANCE AND PUBLIC ADMINISTRATION COMMITTEE

EXPOSURE DRAFT OF THE AUSTRALIAN PRIVACY PRINCIPLES

AUGUST 2010

TABLE OF CONTENTS

1 INTRODUCTION

Microsoft Australia (Microsoft) welcomes this opportunity to offer its perspective on the Australian Privacy Principles (APPs) to the Senate Finance and Public Administration Committee to assist it in its inquiry into Exposure Drafts of Australian Privacy Amendment Legislation.

Microsoft provides this submission as an organisation that is a major provider of software and online services and is conscious of its responsibility to mitigate any associated privacy risks. Indeed Microsoft CEO Steve Ballmer recently noted that:

> As a big company, we've got to lead on privacy.... We have a responsibility, all of us, not just to socially respect the user, but to build the technology that will protect the anonymity, the privacy, the security of what I say, who I say it to, where I go, what's important to me.[1]

This submission is informed by Microsoft's privacy vision; a vision for ubiquitous computing to reflect the need for privacy and data protection so that individuals and organisations can share, use and manage personal information in a trusted computing environment.

The submission is also framed in terms of Australian and worldwide trends since the Australian Law Reform Commission's (ALRC) inquiry reported in *ALRC Report 108 For Your Information: Australian Privacy Law and Practice* (the ALRC report). These trends include rapid changes in and/or adoption of new technologies and in worldwide regulator responses. In particular we are seeing an increased focus on effective compliance and enforcement and improved methods of implementation such as privacy by design.[2] On the Australian front, relevant context includes the introduction of the National Broadband Network (NBN), e-health, health identifiers and increasing use of Internet and mobile devices.

Microsoft has previously provided lengthy submissions to the ALRC and to the Government as it developed its response to the ALRC's report. Both processes have been responsive to many of the issues Microsoft raised. This submission will not repeat those issues or offer a line-by-line analysis of the APPs but rather is intended to take a more strategic approach. Microsoft's overall response to changes to Australia's privacy laws will also depend on measures that are to be dealt with at later stages in the Privacy Law amendment process including any requirements in relation to privacy impact assessments and data breach notification.

In this regard Microsoft notes that the Government is still developing its response to some of the ALRC's recommendations. It urges that priority and resources are allocated to this work. Any slowing down of the implementation of the response could leave Australia in a position of falling behind global initiatives in privacy law reform.

Microsoft sees the proposed changes to Australia's privacy laws as a positive move in enabling individuals, organisations and government to take up emerging ICT opportunities. Microsoft considers that maintaining and developing effective privacy law is a key issue for the Australian economy especially as the NBN is rolled out. In particular, the approach needs to mitigate the current perceived and actual risks for individuals where organisations process or store information offshore.

[1] Speech at the University of Washington about the many benefits that client software and cloud services technology at www.microsoft.com/presspass/exec/steve/2010/03-04cloud.mspx

[2] Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada describes privacy by design as a 'philosophy and approach of embedding privacy into the design specifications of various technologies'. See for www.ipc.on.ca/images/Resources/privacybydesign.pdf

Microsoft urges an approach that is consistent with international privacy approaches such as those emerging in the European Union, the United States, and by the Asia Pacific Economic Cooperation (APEC). Moving unilaterally on privacy regulation will leave Australian companies at a competitive disadvantage.

Microsoft has been a key player in APEC Data Privacy Sub-Group (DPS) that has developed a framework that combines a base-line set of privacy principles and mechanisms to back up assurances of compliance and to facilitate cross border enforcement of a country's privacy rules. Microsoft is also a supporter of processes to harmonise European Union and APEC privacy approaches to cross border privacy rules (CBPR) and is also contributing to the dialogue on reasonable and consistent rules to support law enforcement needs, for example in relation to data retention requirements and access to data under warrant or otherwise.

Microsoft Privacy Principles

- **Accountability** in handling personal information within Microsoft and with vendors and partners
- **Notice** to individuals about how we collect, use, retain, and disclose their personal information
- **Collection** of personal information from individuals only for the purposes identified in the privacy notice we provided
- **Choice and consent** for individuals regarding how we collect, use, and disclose their personal information
- **Use and retention** of personal information in accordance with the privacy notice and consent that individuals have provided
- **Disclosure or onward** transfer of personal information to vendors and partners only for purposes that are identified in the privacy notice, and in a security-enhanced manner
- **Quality assurance** steps to ensure that personal information in our records is accurate and relevant to the purposes for which it was collected
- **Access** for individuals who want to inquire about and, when appropriate, review and update their personal information in our possession
- **Enhanced security** of personal information to help protect against unauthorised access and use
- **Monitoring and enforcement** of compliance with our privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints, and disputes.

Microsoft considers that a stable and consistent base line privacy law, supported by other mechanisms including technology, innovative implementation, sound governance and consumer support mechanisms is the route to effective privacy protection.

2 MICROSOFT AND PRIVACY

Microsoft believes individuals have the right to control their personal information, to be selective about the communication they receive, and to trust the technologies, services, and solutions they use on a regular basis. To this end, Microsoft commits significant resources towards embedding privacy in its culture and products to protect and manage information confidently and safely.

Microsoft was one of the first companies to appoint a chief privacy officer nearly a decade ago. Today we employ more than 40 employees who focus on privacy full-time, and another 400 throughout the company who focus on it as part of their jobs.

We have a strong set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and protects user privacy.

We have made significant investments in privacy training and in building our privacy standards into our product development and other business processes.

The principles of transparency, control, and security have guided our Microsoft approach to privacy.

Transparency is about helping you easily discover and understand how your information is collected and used. This is why the Microsoft Online Privacy Statement appears at the bottom of every Microsoft-owned Web page.

Control means we provide options about how your information is made available to others and used by others.

Security is the notion of protecting your information from harm caused by unauthorized use or disclosure.

Microsoft develops technologies and guidance to enable individuals and organisations to better protect their privacy and reduce the risk of sensitive data loss.

For consumers, we provide privacy-enhancing technologies in our products and services that help protect their personal information.

To help organisations more effectively manage or "govern" the data in their possession, we provide guidance, frameworks, and technologies designed to help protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability.

3 INTERNATIONAL PRIVACY DEVELOPMENTS

Since the ALRC report the world has continued to change rapidly and privacy issues have become more pronounced.

Technology changes noted by the ALRC in 2008 have increased. Widespread access to the Internet and an explosion of online services such as social networks, location based services, and advertising based on online behaviours, are continuing to redefine how personal information is collected, transmitted, and used. When the ALRC reported 120 million people used Facebook. Now it has 500 million users. The evolution of cloud computing also means that data flows are increasingly global, continuous, and delivered to multiple points simultaneously.[3]

These developments offer many benefits and opportunities but also create significant privacy and security challenges for individuals, organisations, and government policymakers.

Businesses in particular are looking for flexible, internationally consistent law that will be cost effective to work with and allow them to reassure their customers that their personal information will be secure no matter where handled. Governments and regulators currently also appear to have more appetite to engage with the issues. There is a range of factors at play here. As well as responding to business interests the agenda is being influenced by changes in the political environment, the fact that data breach rates are huge and not slowing down and some business practices that have come into question.

Internationally regulators are rethinking privacy regulation. These discussions are still in progress and the United States Department of Commerce and the FTC have been conducting consultations on matters such as:

- alternatives to the current “notice and choice” model;
- the pros and cons of using data personal information in new ways for example in behavioural targeting;
- technology issues including cloud computing;
- ID management and accountability; and
- privacy and innovation. [4] [5]

[3] In simple terms, cloud computing is a way to enhance computing experiences by enabling users to access software applications and data that are stored at off-site datacenters rather than on the user’s own device or PC or at an organisation’s on-site datacenter.

[4] See www.ftc.gov/bcp/workshops/privacyroundtables/

The European Union also has improvements in the privacy protection framework on its agenda. Viviane Reding, the European Commission's Vice-President for Justice, Fundamental Rights and Citizenship remarked early in her term "We need to strengthen substantially the EU's stance in protecting the privacy of our citizens".[6] Her colleague Peter Hustinx, the European Data Protection Supervisor, also sees the need for change not so much in the form of privacy laws but in how it is implemented and enforced. He considers that:

- the rights of the citizen won't change much but there will be more emphasis on easier access to exercising existing rights;
- the future will be based on organisations having a stronger incentives to do the right thing by privacy via a combination of commercial reality and regulatory incentive;
- "Law should not legislate on technology" rather organisations should operationalise privacy by design, including more "privacy by default" settings;
- effective accountability will become more important; and
- really getting privacy right will mean not just seeking compliance with privacy law but demonstrating that "all measures have been taken to ensure that compliance will be a result".[7]

While it not clear yet how these various initiatives will play out or whether they will result in a more convergent approach to privacy protection, a common theme, also reflected in the ALRC report and now in the APPs, is the increasing emphasis regulators and lawmakers are placing on the need for accountability, including when information travels between jurisdictions.

Recently the European Union Working Party set up under Article 29 of Directive 95/46/EC recommended a new principle on accountability which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

It also seems that there is increasing emphasis on regulatory cooperation. While regulators worldwide have taken a while to recognise the full privacy implications of electronic data transfer, they are now taking concerted steps to address gaps in the effective protection of individuals. For example, the APEC Cross-Border Privacy Enforcement Arrangement (CPEA) will enable privacy regulators to give and obtain assistance from foreign privacy enforcement authorities to resolve complaints against overseas companies.[8] The CPEA is a structured regional arrangement, setting out specific procedures and mechanisms for cooperation among participating privacy enforcement authorities in APEC member economies.

The comments here are not intended to be a comprehensive survey of all current international privacy developments, rather they are intended to point to the importance of Australia's continued

[5] US privacy lawyers Hunton and Williams provide an overview of the Department of Commerce initiative www.huntonprivacyblog.com/2010/05/articles/centre-for-information-policy-2/commerce-department-takes-lead-in-developing-us-internet-privacy-framework/#more

[6] See Ms Reding's speech at http://ec.europa.eu/commission_2010-2014/reding/pdf/mandate/reding_speaking_points_media_summary.pdf

[7] See www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf

[8] For information about the CPEA see www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce/cpea.html

engagement with the issues. Microsoft supports effective regulation. It considers that Australia must be mindful of the volatile international environment and stay well in touch with these developments.

4 COMMENTS ON THE AUSTRALIAN PRIVACY PRINCIPLES (APPS)

Microsoft indicated in its submission to the ALRC Discussion Paper 72 that it recommended a law that is:

- principles based;
- technologically neutral;
- harmonised at both an international and national level; and
- that is conducive to innovation.

Microsoft considers that in general the APPs are consistent with these criteria. We are pleased to see the increased emphasis on transparency and compliance assurance and supports the refined approach to cross border disclosure of personal information. However, there is potential for more effective implementation, cost reduction or facilitating innovation. We also have some thoughts on the concept of accountability that is introduced in APP 1 as an explicit obligation to take steps to comply, and in APP 9 as a requirement to take reasonable steps protect personal information where it is disclosed to organisations outside of Australia.

Microsoft supports the approach of organising the principles in terms of the personal information life cycle, and would support further simplification of the drafting where possible. Microsoft encourages consistency in the structure of the APPs. It notes, for example, that APP 1 is the only principle that has an object.

As noted above, this submission does not offer a line-by-line analysis of the APPs but will focus on some strategic issues that Microsoft has identified. However, the fact that Microsoft has not commented on a provision does not necessarily indicate its agreement with the provision.

4.1 TECHNOLOGICAL NEUTRALITY

Microsoft welcomes the commitment in the *Government's Companion Guide to the Australian Privacy Principles* (the Companion Guide) to maintaining technological neutrality as a key concept for the APPs. However, it remains to be seen whether this commitment is carried through in the drafting of the remaining sections of the Exposure draft and the Government's response to the ALRC recommendations that are yet to be considered.

As indicated in its submissions to the ALRC, Microsoft does not think that it is appropriate for the Minister to prescribe privacy and security standards for certain technologies as suggested by the ALRC in Proposal 7-2. It considers that such an approach has the real potential to stifle innovation and to damage Australia's attractiveness as a test market.

As the remaining parts of the Government response and exposure drafts are released Microsoft will be hoping to see measures that will allow and support market forces as the driver for best practice. We expect these measures could include data breach notification and other sanctions or incentives but are be wary of an ability to prescribe standards for particular technologies.

4.2 DEFINITION OF PERSONAL INFORMATION

The Exposure Draft includes an amended definition for personal information. The Companion Guide advises that "the key conceptual difference revolves around the concepts of "identity" as used in the current definition, and "identification" as referred to in the recommended definition. The ALRC

considered that "identification" is more consistent with international language and international jurisprudence, and that explanatory material based on the terms "identified" and "identifiable" will be more directly relevant".

Microsoft is not entirely in agreement with the view in the Companion Guide that the proposed definition does not significantly change the scope of the existing concept in the Privacy Act. However, if the changes are merely cosmetic then it is not clear that there is an argument for change. Even minor changes in the law will require organisations to consider their personal information holdings, and their policies and documentation with consequent compliance costs.

That said Microsoft welcomes the comments in the Companion Guide that the "reasonable" test limits apply based on the context and circumstances. Microsoft agrees that while it may be technically possible for an entity to identify a person by the information it holds, it may be that it is not practically possible (for example due to logistics, legislation or contractual restrictions). Microsoft would welcome further clarification of the application of the definition in any guidance material produced by the Office of the Privacy Commissioner (OPC) or the Office of the Information Commissioner (OIC) (which will incorporate the OPC from November 2010).

4.3 APP 1—OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION AND APP 5—NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

APP 1 sets out measures that together are intended to promote the open and transparent management of personal information. These measures are:

- a new requirement for organisations to take reasonable steps to implement practices, procedures and systems to ensure they comply with the APPs and to enable them to respond to privacy complaints and
- a requirement to have a privacy policy that addresses certain matters and to take reasonable to make it available, including, if requested, in a specified form.

APP 5 sets out the matters that organisations are required to tell individuals at or before, or as soon as practicable thereafter, personal information is collected. In summary these matters are:

- the identity and contact details of the entity;
- if not likely to be known, including because the information was collected from someone else, that information has been collected and the circumstances;
- if the collection is authorised by law;
- the main purposes for which personal information is collected;
- the main consequences if any if the information is not provided;
- to whom the information is usually disclosed;
- that information about access, correction and complaint processes can be found in the organisation's privacy policy; and
- if the personal information will be disclosed overseas, and if so, if practical to specify, where.

4.3.1 COMPLIANCE REQUIREMENT (APP 1.2)

Microsoft does not believe there is any need for the proposed APP 1.2. Section 16A of the *Privacy*

Act 1988 (Cth) (the Privacy Act) provides that "an organisation must not do an act, or engage in a practice, that breaches a National Privacy Principle". Assuming that a modified version of this obligation will be enacted to prohibit breaches of the APPs, regulated entities will, as a matter of practice, need to take steps to ensure that their conduct will comply with the APPs. If APP 1.2 was enacted as proposed, it would be possible for an entity to be liable for breaching APP 1.2 simply because it had not prepared a document that described the procedures it would take with the objective of ensuring compliance with the remainder of the APPs. This would be so even if there had been no breach by the entity of any of the substantive APPs.

Microsoft's approach is to monitor and enforce compliance with our privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints, and disputes. In our experience, this approach is taken by almost all businesses we deal with. So, we are not against the development of appropriate and effective measures to ensure that privacy principles are complied with. We just do not believe that APP 1.2 will assist individuals whose privacy is at risk of being interfered with - they will have remedies if and when a breach of the substantive principles occurs. In a case involving serious and systematic breaches of the APPs, a court has power under section 98 of the Privacy Act to require an entity to take positive steps to prevent future breaches. This power would likely extend to introducing a compliance program - similar orders are commonly made at the request of the ACCC in cases involving contraventions of the *Trade Practices Act*.

4.3.1.1 PRIVACY BY DESIGN

The Companion Guide notes that the "principle is intended to outline that part of complying with the APPs is making sure that entities consider their privacy obligations when planning new systems – this part of the International moves towards 'privacy by design' approach that is ensuring that privacy and data protection compliance is included in the design of information systems from their inception".

Microsoft considers that it could be hard to read privacy by design elements into the principle as currently worded. Moreover, it is wary about loading this concept into the principle. It is difficult to see how such a requirement would be defined or enforced and it raises real possibilities of inappropriate government interventions into what should properly be business decisions. Microsoft also notes that the EU Data Protection Supervisor, Peter Hustinx, has expressed the view that privacy by design would not be a matter of law but rather would be achieved through the practices of organisations. The US Department of Commerce also seems likely to reach this conclusion. Microsoft agrees strongly with these views. It considers that legislating for privacy by design would be onerous, impractical and would have real potential to stifle innovation. It suggests that a more fruitful path would be to explore options for regulator support and encouragement and possible incentive programs.

4.3.2 PRIVACY POLICY REQUIREMENTS (APPS 1.3 – 1.6) NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION (APP 5)

The proposed APP 1.4 lists the matters a privacy policy should address and adds requirements in addition to those listed in current National Privacy Principle (NPP) 5. These include telling people about the organisation's access, correction and complaint processes and, if practical, if the organisation discloses personal information to overseas recipients where those recipients are likely to be located.

A privacy policy requirement is also a common feature in most, if not all, international privacy frameworks. Microsoft also notes that the Privacy Act, in both the NPPs and the APPs, takes a belt and braces approach to transparency with requirements both for a privacy policy and for individuals to be advised of certain matters at the point at which personal information is collected (NPP 1.3 in the

current Privacy Act and APP 5). Where the Australian transparency approach is starting to diverge from other frameworks in the extent of matters that the policy and notices should address.

Microsoft appreciates that there are good arguments for individuals to be aware of each of the matters listed in APP 1.4 and APP 5. However, it also notes that there is an increasing body of thought and experience concluding that requirements to give notice lead to lots of notices but not necessarily to more power or choice for individuals. In fact, there is evidence that individuals can be overwhelmed but not enlightened by long privacy policies or disclosure statements, even where intended to allow informed consent. This emphasis does not take into account the realities of the way high volumes of personal information are collected used and disclosed in the current and rapidly evolving IT environment let alone the continued aggregation and sharing by third parties. It leaves individuals users bearing the risk in circumstances where they are not equipped, and as research is showing, not willing, to bear it[9]

At a practical level, Microsoft's experience is that it can be difficult to work out how the policy and notice obligations relate. Our observation is that organisations have often tended to focus on the privacy policy and so may not be meeting the strict requirements of the notice obligations. The Exposure draft makes a clearer link between the privacy policy and notices requirements at least in relation to the location of detail about access and complaint processes. APP 5 also introduces some welcome flexibility by allowing organisations to decide that in a particular set of circumstances it would be reasonable not to take any steps to provide notice.

However, in Microsoft's view more could be done. One approach to resolving the matter would be to recast APPs 1.3 – 6 and APP 5 into a layered notice format. Some years ago privacy regulators globally endorsed this approach as a means of making it easier for individuals to understand why personal information is being collected. The approach was based on the understanding at the time as to better communication practices. **[10]** However, even this approach is now being challenged with more recent research suggesting, for example, adopting practices used in the food-labelling context could be a more effective way to go.[11] Other research suggests that effective messaging is possible with tools such as "visceral notice" and anthropomorphic cues.[12]

It should be noted that Microsoft was one of the first companies to develop so-called "layered" privacy notices that give clear and concise bullet-point summaries of our practices in a short notice, with links to the full privacy statement for consumers and others who are interested in more detailed information.

Microsoft concludes that it would be desirable to combine and streamline the specific requirements in APPs 1.3 – 6 and APP 5 by focussing on identifying transparency objectives. This would leave scope for organisations that so chose, possibly in consultation with regulators and on the basis of context to

[9] See "The Failure of Fair Information Practice Principles" by Professor Fred Cate in *Consumer Protection in the Age of the 'Information Economy'*, Amazon reference *www.amazon.com/Consumer-Protection-Information-Economy-Markets/dp/0754647099*

[10] The Multi Layered Privacy Notices format is based on a recommendation of the Privacy Commissioner in Recommendation 19 and 20 of Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 available at www.privacy.gov.au. These recommendations support the development of short form privacy notices. Multi-Layered Privacy Notices were also endorsed by Data Protection and Privacy Commissioners in 2003, further developed in the Berlin Memorandum, and endorsed in Opinion WP 100 by the Article 29 Committee of European Data Protection and Privacy Commissioners. See Privacy Notice Resolution Resources (International Conference of Data Protection & Privacy Commissioners (25th Sydney, 2003). Multi-Layered Privacy Notices are based on the work of the Center for Information Policy Leadership.

[11] Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach", Cranor et al, CyLab, Carnegie Mellon University at http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html

[12] "Redrawing the Route to Online Privacy", NY Times, 28 Feb 2010 www.nytimes.com/2010/02/28/technology/internet/28unbox.html?_r=1

decide how best to communicate with individuals to meet these objectives in an effective and cost efficient way. Microsoft would expect that a detailed privacy policy document would still be available to interested individuals and professional advisors or commentators, and also that for organisations whose business model relied more on certainty than innovation that the more conventional policy/notice route would still be available.

This would help reduce the compliance burden on organisations and reduce the load on individuals. Microsoft acknowledges that getting to this outcome will require insightful education and engagement by policy makers, lawmakers and regulators.

4.4 APP 8—CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

Microsoft understands that the APP 8 reflects some key changes in approach to cross-border disclosure of personal information. In particular APP 8:

- refers to disclosure rather than transfer (which is used in the existing NPP 9);
- moves from a model where transfer is prevented unless a specific exception applies to a model that permits disclosures to proceed provided that, unless an exception applies, the organisation remains responsible or accountable (through the application of section 20) for the personal information, including by being held legally responsible for any interference with an individual's privacy;
- strengthens the protection for individuals where the organisation seeks to disclose information on the basis that the overseas recipient is subject to a law or binding scheme that is at least substantially similar to the Privacy Act by adding a requirement that the law or scheme need to include a redress mechanism that the individual can access; and
- includes a range of new exceptions which are intended to ensure federal agencies can continue to disclose personal information to overseas recipients for public interest purposes.

Microsoft is on the record of supporting the APEC accountability principle. However the combination of APP 8 and section 20 appears to go further than both the APEC accountability principle and the government's own response to the ALRC's recommendations.

The APEC framework requires controllers of personal information to either obtain consent to data exports or to "exercise due diligence and take reasonable steps to ensure the recipient person or organisation will protect the information consistently" with applicable privacy principles. However, the proposed section 20 goes further by providing that the Australian entity will be liable to Australian individuals if the recipient outside Australia acts inconsistently with the APPs. Liability will be imposed even where the Australian entity exercised due diligence and took reasonable steps to ensure that the recipient would abide by the principles.

The government's first stage response to the ALRC's recommendations (see pages 77 and 78 of 144) contemplates that accountability will be imposed on the Australian data exporter unless the recipient "is subject to obligations to uphold privacy protections substantially similar to the [Australian] privacy principles and where there are accessible mechanisms for individuals to take effective action to have the privacy protections enforced". The government considered that those enforcement mechanisms may be expressly included in a law or binding scheme or may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate foreign regulator. The exposure draft APP 8.2(a) does not appear to reflect this position.

Therefore Microsoft is of the view that APP 8.2)(a) should be replaced or reworded to reflect the following:

- the foreign recipient is in a jurisdiction with an adequate level of protection;
- the foreign recipient is in a jurisdiction that has entered into a cross border enforcement arrangement with the OPC that will enable an individual to pursue a claim against the foreign recipient in respect of conduct that would constitute an interference of privacy if it had occurred in Australia.

Microsoft also considers that there should be a positive obligation on the Privacy Commissioner to identify those jurisdictions that afford an adequate level of protection.

4.5 APP 11—SECURITY OF PERSONAL INFORMATION

APP 11 includes similar obligations for organisations as the current NPP 4.

Microsoft views security as an absolutely critical element of a privacy framework. Poor security makes privacy impossible. Getting security right is a bit more objective than some other aspects of privacy and could accommodate some more specific tests provided these did not affect cost effectiveness and were conducive to innovation.

In its submissions to the ALRC process, Microsoft called for the inclusion of a specified list of factors in the data security principle to help guide any determination as to whether an organisation has taken "reasonable steps" to secure personal information it holds.

Microsoft reiterates its view that it would be preferable to include this list of factors in the Privacy Act itself. However, if the Government is not inclined to adopt that approach, then Microsoft would also support the inclusion of those factors in guidance issued by the OIC.

Microsoft Australia looks forward to working with the Senate Finance and Public Administration Committee on the Australian Privacy Principles.

CONTACT

Please address any questions regarding this submission to:

Sassoon Grigorian
Manager, Government Affairs
Microsoft Australia
1 Epping Rd
North Ryde NSW 2113