Macquarie Telecom Pty Ltd
Level 20, 2 Market Street
Sydney, NSW 2000

Call 1800 676 272
Fax 1800 676 373

ABN 21 082 930 916

23 July 2012

Committee Secretary
House of Representatives Standing Committee on
Social Policy and Legal Affairs
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email spla.reps@aph.gov.au

Dear Sir/Madam

MACQUARIE TELECOM PTY LIMITED – SUBMISSIONS TO STANDING COMMITTEE ON SOCIAL POLICY AND LEGAL AFFAIRS INQUIRY INTO THE PRIVACY AMENDMENT (ENHANCING PRIVACY PROTECTION) BILL 2012

Macquarie Telecom Pty Limited (**Macquarie**) welcomes the Government's announcement that the Standing Committee on Social Policy and Legal Affairs (**Committee**) will conduct an inquiry (**Inquiry**) into the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (**Bill**).

Macquarie is Australia's leading provider of managed hosting services and business-only telecommunications company. Macquarie is based in Australia and provides hosting and cloud services with no offshore components and leads a new industry coalition to build Australian consumer and business confidence in cloud computing. Macquarie has a depth of experience in the communications sector which means it is well positioned to provide comment on the Bill.

Attorney-General Nicola Roxon has stated that the Bill represents “the most significant development in privacy reform since Labor introduced the Privacy Act in 1988”; and that “these new privacy laws focus on giving power back to consumers over how organisations use their personal information.”[1] However, Macquarie is concerned that some of the proposed amendments may have the unintended consequence of resulting in worse outcomes for privacy protection than the current regime. If these issues are not adequately addressed, there is a real risk that the proposed changes will in fact be a 'step backwards' for individuals and privacy protection.

This letter sets out Macquarie's primary concerns with the Bill which largely relate to cross border disclosure of personal information. This letter also sets out pragmatic and easy to implement recommendations to deal with this unintended consequence. The recommendations ensure the principles of the Bill are appropriately structured in order to better meet the Government's core objective of strengthening privacy protection for Australians.

[1] The Hon Nicola Roxon MP, Attorney General for Australia in 'Privacy Reform Laws Introduced into Parliament', 23 May 2012 available at http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/23-May-2012---Privacy-reform-laws-introduced-into-Parliament.aspx

1. Australian Privacy Principle 8 (APP 8)

1.1. Change of terminology from 'transfer' to 'disclosure' may have the unintended effect of diminishing protection in certain circumstances

Macquarie welcomes the inclusion of the term 'disclosure' in APP 8. However, Macquarie is extremely concerned that the proposed APP 8 as currently drafted may result in diminished protection in certain situations where information is 'transferred' offshore but not 'disclosed' to an overseas recipient. Accordingly, the APP 8 should be amended to refer to both 'transfer' and 'disclosure'.

The Explanatory Memorandum states that APP 8 would not apply to 'overseas movement of personal information if that movement is an internal use by an entity, rather than a disclosure.' One example where personal information may receive inferior protection under the proposed APP 8 compared with existing National Privacy Principle 9 (**NPP 9**) is where an entity is using a private cloud overseas.

In this circumstance, where the organisation has exclusive use of cloud infrastructure and services, it may 'transfer' but not 'disclose' information by storing it, using that infrastructure. Macquarie submits that such 'transfer' movements of personal information should be expressly regulated by APP 8 to ensure that individuals are no worse off under the new regime.

Even if an overseas jurisdiction offers substantially similar protections of information to that provided by the APPs, the act of transferring an individual's information to an overseas jurisdiction is likely to expose that information to disclosure to government agencies and others within that jurisdiction and accordingly such transfer should only occur with the consent of the affected individual.

1.2. Even where an entity has a reasonable belief that the overseas recipient is subject to obligations which protect information in at least a substantially similar way to the protection provided by the APPs, the entity should be required to seek consent to cross border disclosure of personal information

Macquarie submits that it is important that the Committee carefully review the exceptions to the new accountability approach to cross border disclosure of personal information in APP 8.1 and section 16C. APP 8.2(a) creates an exception where a disclosing entity reasonably believes privacy obligations applying to the overseas entity by virtue of law or binding scheme are substantially similar to the protections provided by the APPs and the individual has access to overseas law enforcement.

This exception effectively shifts the burden of non-compliance by the overseas entity from the Australian entity to the individual. In its current form APP 8.2(a) would permit disclosure in the absence of consent from that individual.

Macquarie submits that the requirement for the Australian entity to ensure the overseas entity is subject to substantially similar obligations in relation to protection of personal information should be combined with a requirement that the Australian entity seek consent from the individual to cross border disclosure of personal information. The additional protection contained in APP 8.2(a) that there must be accessible mechanisms which allow the individual to enforce those protection obligations may be rendered virtually redundant where an individual is not aware that their personal information has been disclosed to an overseas recipient in a particular instance. In any case, it is likely to be difficult for an affected individual to avail themselves of the law enforcement mechanisms available overseas where limited visibility of data flows in the global cloud may mean it is impossible to determine which jurisdiction the data is in at any one time. The severe curtailment of effective enforcement options for affected individuals where personal information is mishandled overseas is expressly recognised in the Explanatory Memorandum to the *Personally Controlled Electronic Health Records Act 2012* (Cth) (**PCEHR Act**).[2]

Macquarie supports the requirements, contained in APP 5.2(i) and 5.2(j) for an entity to notify individuals of whether it is likely to disclose information to overseas recipients and the location of those likely recipients. However, more robust protection is required with respect to discrete transfers which are not considered 'likely' at the time of collection (and therefore do not attract APP5.2(i) and (j)).

As it is currently drafted, APP 8.2(a) provides for the individual to lose the right to hold the Australian entity accountable for acts done by the overseas entity which would constitute a breach of the APPs. Macquarie submits that it is inappropriate that the individual is not given the opportunity to reject disclosure to an overseas entity in these circumstances.

Macquarie submits that the requirement that the entity seek consent, combined with the disclosure notification obligations in APP 5.2(i) and 5.2(j) will provide more robust protection for individuals in circumstances where they will not have recourse to the Australian entity under section 16C and where disclosure to the overseas entity may not be considered likely at the time of collection so as to attract the operation of the obligations contained in APP 5.2.

1.3. Where the laws are not substantially similar to the protection provided by the APPs, the entity should be required to expressly inform the individual of this 'non-equivalence' and obtain express consent to the 'non-equivalence'

Macquarie submits that where an entity is relying on individual consent to disclosure pursuant to 8.2(b), the entity should be required to expressly inform the individual that the information will not be subject to protections which afford substantially similar protection to that contained in the APPs, in addition to the warning currently required by 8.2(b)(i) that consent will result in APP 8.1 being inapplicable to that disclosure. As part of this consent process, the entity should be required to identify the specific areas of 'non-equivalence' and obtain the individual's specific consent to such 'non-equivalence'. Robust privacy laws requires that individuals are appropriately informed before they provide their consent to such off-shore disclosure.

[2] Explanatory Memorandum, PCEHR Act, page 49.

In this respect, Macquarie refers to the Explanatory Memorandum to the Bill. The Explanatory Memorandum states that '[APP 8] will aim to permit cross-border disclosure of personal information and ensure that any personal information is still treated in accordance with the Privacy Act.' APP8.2(b) is an exception to the accountability approach and deprives the individual of the protection created by section 16C. Where an entity is relying on individual consent for cross border disclosure of information, that entity should be required to take steps to ensure the individual is aware not only that the Privacy Act will not apply but that the entity does not believe the overseas recipient is subject to any equivalent regime and to give the individual the chance to refuse disclosure.

1.4. An objective test should apply to the legal or binding obligations on the overseas recipient to protect information

Related to the above point, the Committee should be directed to have regard to the fact that the 'reasonable belief' test contained in APP 8.2(a) allows entities to make unilateral decisions in relation to cross border disclosure of personal information based on a subjective belief about information available to them and the context of a particular disclosure. Specifically, the Committee should have regard to the fact that this exception erodes the new accountability approach to cross border disclosure of personal information.

If the Australian entity is to be exempt from the requirement to 'take reasonable steps' in APP 8.1(a) and therefore exempt from continued liability for mismanagement by the overseas entity in section 16C, the test for whether the overseas recipient is subject to substantially similar obligations should be objective. This is even more critical if the Committee does not adopt Macquarie's recommendation at 1.2 that consent be an additional requirement in relation to the exception contained in APP 8.1(a).

2. Government agencies

2.1. Personal information collected by public sector agencies should be held onshore

A potential risk of the Bill is that the creation of a unified set of principles to apply to both private sector organisations and public sector agencies will fail to reflect the different expectations Australian consumers have as to how agencies will handle their personal information. This is highly undesirable.

Macquarie submits that individuals have a higher expectation of public sector agencies and their handling of personal information. Accordingly, a higher standard is required for government agencies in relation to certain aspects of handling personal information, specifically to cross border disclosure of personal information which is regulated by APP 8.

Macquarie refers the Committee to section 77 of the PCEHR Act. The PCEHR Act prohibits operators or service providers from holding, taking, processing or handling outside Australia records which contain personal information about consumers or participants in the PCEHR system. The Explanatory Memorandum to the PCEHR Bill recognises the policy decision to require all PCEHR information to be stored and processed in Australia is based on the following risks: lack of effective enforcement options available where information is misused or mishandled; curtailment of remedies for affected individuals; and the increased risk of information being compulsorily acquired by foreign governments.

The Australian public has an expectation that data collected by public sector agencies will be held onshore and not disclosed to offshore entities. This expectation is widely recognised, and is reflected for example by NBN Co, a wholly owned Commonwealth company and prescribed Government Business Enterprise[3], requiring those tendering to provide services to NBN Co to use onshore data hosting facilities.

The exceptions to cross border disclosure contained in APP 8 are not appropriate for public sector agencies. As it has done with the PCEHR system, the Government should insist on local data centres for all personal information collected by its agencies. In Macquarie's opinion, the Australian public has an interest in consistent privacy protections across all information held by Government agencies.

2.2. At a minimum sensitive information collected by public sector agencies should be held onshore and not transferred off-shore under any circumstance

Macquarie supports the distinction drawn between personal information generally and personal information that is sensitive information in relation to collection in APP 3. For the reasons set out above that sensitive information should be subject to more stringent regulation. Put simply, sensitive information held by public sector agencies should never be held or disclosed offshore.

2.3. Very specific consent in respect of non-sensitive personal information

Given the above, it is imperative that the Bill be amended so that a higher standard of care is imposed on public sector agencies in relation to cross border disclosure of personal information. If APP 8 is to permit the disclosure of personal information by agencies to overseas entities, the exceptions contained in APP 8.2 should be tailored appropriately.

As submitted in section 2.2 above, sensitive information should never be held or disclosed offshore. Further, Macquarie submits that where a government agency wishes to store or disclose non-sensitive personal information off-shore, that government agency should be required to obtain an express and specific consent in respect of such disclosure or storage.

APP 8.2 contains two exceptions which limit accountability for cross border disclosure of personal information. According to APP 8.2(b), the entity is able to disclose information to an overseas entity if the individual consents to the disclosure after having been informed that the protections in APP

[3] *Commonwealth Authorities and Companies Act 1997* (Cth).

8.1 will not apply. The Bill proposes to retain the existing definition of 'consent' contained in the *Privacy Act 1988* (Cth). Consent is defined to mean 'express consent or implied consent'. This may have the consequence that the individual loses the right to hold the agency liable through implied or bundled consent.

For the reasons set out above, Macquarie submits that express consent should be required where an agency purports to disclose non-sensitive personal information to an overseas entity.

Macquarie submits that the exception contained in APP 8.2(a) should be confined to organisations. If APP 8.2(a) is to apply to agencies, for the reasons set out here and in 1.2, the agency should be required to seek express consent from the individual. Individuals should have the ability to control the management of their personal information by agencies and have the opportunity to choose whether information is disclosed to an entity not located within Australia's territorial boundaries.

Macquarie welcomes the opportunity to participate in the Inquiry and would be pleased to engage in further dialogue with the Committee as it progresses this important work.

Macquarie supports the Government's objective of strengthening privacy laws. However, if the issues set out in this letter are not adequately addressed in the final Bill there is a real risk that the Bill will not provide for adequate protection of personal information of the Australian public. In fact, there is a real risk that individuals may be worse off in certain circumstances under the proposed Bill.

These risks could be easily addressed by implementing Macquarie's pragmatic recommendations as set out in this letter.

Please direct any queries regarding this submission to the undersigned.

Yours sincerely

Matt Healy
National Executive – Industry & Policy

[redacted]