Senate Finance and Public Administration Committee
Invitation to provide submissions on the
Australian Privacy Principles Exposure Draft
("Exposure Draft")

Submission by Telstra Corporation Limited – August 2010

* * *

Telstra welcomes the opportunity to provide comments on the Exposure Draft.

We set out below our responses on specific topics.

We also make this submission on behalf of our wholly owned subsidiary, Sensis Pty Ltd.

General comment

We commend the Government's policy objectives in introducing a single, national set of privacy principles for Australia in the form of the Australian Privacy Principles ("APP"s). We recognise the importance for consumers to have consistent standards applied to the protection of their personal information. We commend the APPs drawing on the existing standards in the National Privacy Principles ("NPP"s) and aiming to produce a set of standards that strikes a balance between the sometimes competing interests of Government, business, law enforcement and consumer protection. Telstra welcomes the opportunity to share our perspectives and suggestions on the development of a balanced single national privacy law.

Specific issues raised in the exposure draft

1. Proposed APP 1 (open and transparent management of personal information)

We suggest that the notice requirement in (1)(4)(g), to list the overseas countries where personal information is likely to be disclosed, should be removed.

Since contractual outsourcing arrangements in the business world may change frequently, this requirement would necessarily have to be satisfied by very broad references and catch-alls in a privacy notice. This would diminish the value of providing this information and potentially simply confuse rather than inform consumers.

2. Proposed APP 4 (receiving unsolicited personal information)

APP3 and APP4 could be merged into one principle, with the focus on the particular purpose for which personal information is collected rather than the circumstances of its collection. Alternatively, we propose that APP4 be amended to focus on "passed along" information rather than the concept of "unsolicited" information.

We agree that an entity should not retain personal information that it does not require. However, APP 4 introduces a new concept of unsolicited personal information which highlights two issues.

First, under APP4 an entity's obligations in respect of unsolicited information are the same as the obligations in respect of solicited information, unless the entity could not have collected the information in accordance with the APPs. APP11 already provides that an entity should destroy any personal information that is no longer required for a purpose permitted by the APPs. In light of that we suggest that this form of APP4 does not provide any additional protection over a consumer's personal information so is not required and should be removed. In fact APP 4 would increase the compliance burden upon entities to take steps to identify and distinguish between solicited and unsolicited information, rather than upon whether information in its possession, however collected, is necessary and relevant for its purposes.

An alternative function for APP4 would be to focus on personal information that is "passed along" from an individual or entity to a different entity. It could ensure the pass along entity has the authority to do so and provides the receiving entity with the purpose for which the personal information may be used or disclosed. This would ensure that an entity receiving information being "passed along" has been given proper assurances by the first entity that the individual consented to that information transfer and the purposes for which that information may be used.

3. Proposed APP 5 (notification of the collection of personal information)

Telstra seeks clarification on whether this would require notification of the relevant matters every time we undertake a collection activity. We submit that proposed APP 5 should be amended to clarify that an entity may comply with its notification obligations by having a compliant privacy policy and taking reasonable steps to bring that privacy policy to the customer's attention.

As a matter of practice most organisations (including Telstra) comply with NPP 1.3 by maintaining a comprehensive privacy policy and communicating that policy at the time of collection or as soon as practicable afterwards. We agree that by the APP 1 requiring additional information be disclosed and the policy be kept up to date, the effectiveness of the privacy policy as the primary means for an entity to communicate to individuals how it deals with their personal information is confirmed.

However it is not clear whether APP 5 would be met by prominently bringing the privacy policy to the individual's attention once, or whether the entity must take steps to notify the individual of collection (and relevant matters) each time any of their personal information is collected. This is particularly so because of the introductory wording of this APP (that seems to contemplate individual notices) as compared with the wording of (1)(b) that contemplates awareness of how personal information is used (which would be ongoing after the first notification).

This could translate into entities having to provide a privacy statement notification to a consumer each time the customer interacts with the entity. For example, our standing processes require our staff to check and update a customer's details as an initial step in every transaction and for authentication purposes. This could involve receiving new contact details or email address. It would be unworkable if APP5 required us to provide the notification in every instance. In all likelihood customers would become more dissatisfied as a result of constantly being "bombarded" with copies of an entity's privacy collection statement.

Rather than requiring an ad hoc collection statement each time any personal information is collected we suggest it would be more effective to provide individuals with a comprehensive statement of the entity's privacy policies at the start of the relationship.

4. Proposed APP 7 (direct marketing)

This new APP includes a requirement to obtain an individual's consent before using or disclosing personal information about them that is obtained from a person other than the individual. This seems overly broad in that it would require consent to use publicly available information, consent to use updated information provided by an authorised representative on a customer's account, as well as consent to use updated information obtained by contractors or agencies who carry out certain functions for an entity on its behalf (eg. mailing or telemarketing operations).

This provision should be revised to include the same "would not reasonably expect" wording at the end of (3)(a)(ii) and exclude information obtained from authorised representatives and third parties working for or affiliated with the entity.

Further, the requirement in s.3(d) to provide a statement in each direct marketing communication that the individual may make a request to not receive direct marketing from the organisation would not be required for customers who have already received the entity's privacy statement that has set out this information. Rather, the requirement should only apply where the entity is using or disclosing information about individuals that it does not have a business relationship with and thus who have not already been provided with the entity's Privacy Statement.

5. Proposed APP 8 (cross-border disclosure of personal information)

We recommend that cross-border information flow should not extend to situations where information is not transferred overseas but merely "viewed" overseas.

It seems from the change of terminology from "transfer" to "disclose" in the APPs and the comments in the Companion Guide that a cross-border disclosure will occur when information is accessed by an overseas recipient.

In our experience there is a significant difference between a person overseas being able to temporarily view personal information (without the ability to save, copy or print it locally), and that person being able to have possession of the personal information. In the latter case, we agree that it is appropriate, as it always has been under the NPPs, that the transborder data flow provisions should apply. However, in the case where information is not transferred overseas, but is merely "viewed" overseas, the entity which retains possession of the information should remain responsible for the privacy of the information to individuals. We recommend that there is no reason to extend the application of the transborder data flow provisions to deal with the situation.

We suggest that the Privacy Commissioner provide a list of countries whose privacy laws are substantially similar to Australian laws.

APP8(1) does not apply to the disclosure of personal information to an overseas recipient if the entity reasonably believes that the overseas recipient is subject to

a law or binding scheme that has the effect of protecting the information in a way that is, overall, at least substantially similar to the APPs, and that there are available enforcement mechanisms. As a matter of practice, it would be extremely difficult for entities to make this determination. Of particular concern is the situation where different entities come to different views as to the effect of a privacy law in the relevant jurisdiction.

If the Act were to require the Privacy Commissioner to publish a list of countries that meet the criteria in APP8(2) it would help to ease the compliance burden, particularly for companies without the resources to undertake proper due diligence on the effectiveness of other countries' privacy laws. It would also lead to a more consistent treatment of the protection of personal information between entities. We suspect that the newly formed APEC Cross-border Privacy Enforcement Arrangement would help to facilitate the compilation of such a list, at least in respect of APEC countries.

We propose that the operation of APP8 and section 20 be clarified so they do not extend to information where that information has been made publicly available in a way that is otherwise permitted by the APPs.

We have a concern that APP8 and Section 20 might apply to personal information that is published in a way that is otherwise permitted by the APPS. This would have the effect of making an entity that has lawfully published personal information liable for the actions of any overseas recipient who might access or view that information, unless the recipient is itself subject to the APPs. For example, the White Pages® directory is published in both print and online formats. Once the directory is published, the use that any person (particularly overseas) may make of the information is entirely outside our control. This issue would extend to any entity that published personal information on its website for a legitimate purpose.

6. Proposed APP 11 (security of personal information)

We suggest the removal of the newly inserted concept of "interference".

The concept of "interference" is a new one and it is not clear what activity it is intended to capture, which is not already satisfactorily covered by the existing words 'misuse', 'loss' or 'unauthorised access, modification or disclosure'. It tends to suggest "unlawful interception" which may require degrees of encryption to protect against – this outcome would certainly not maintain the expressed objective of the APPs being technologically neutral and would potentially unfairly impose responsibility for external events or attack.

7. Proposed APP 13 (correction of personal information)

We recommend that APP 13 be amended so that a notice of refusal to correct information is only required to be in writing if requested.

In our experience a refusal to correct information is often quite straight forward and a verbal explanation of the reasons would be sufficient. For example we regularly receive requests from individuals to change their residential listings in the White Pages® directory. However, if those individuals are customers of other carriers/carriage providers, we rely on the information received from the various carriers and carriage service providers for inclusion in the White Pages® directory. If a customer of another carrier contacts us to change their White Pages® directory listing, we generally advise them to contact their carrier to make these changes (who will then send a further listing instruction through to

Sensis) as only their carrier has the necessary account specific information to verify the individual before making any changes to their account listing. There would be little benefit to the individual in us having to provide this reasoning in writing. In fact it would slow down the process and more than likely inconvenience the person while increasing the compliance burden on us.

8. Section 19 (extra-territorial operation of this Act etc)

We propose that the definition of "Australian link" should be amended so that the Act only applies to the personal information of individuals located in Australia.

Section 19(2) provides that the Act (and any approved privacy code) extends to acts and practices outside Australia by an organisation with an Australian link. Given the broad definition of "Australian link", it appears that the APPs would apply to the acts of an overseas company in processing personal information of overseas individuals who have no link to Australia, merely because the company has an Australian branch. This could also result in different, possibly conflicting, laws applying in other jurisdictions.

We propose that section 19 be amended so that the Act and any codes only apply where the relevant personal information is information about individuals located in Australia. The definition of Australian individual could be similar to the existing one in s 5B(1)(a) of the Act.

9. Section 20 (Acts and practices of overseas recipients of personal information)

We suggest that section 20 be amended to replace deemed liability for overseas disclosure with a responsibility to take steps to rectify breaches by overseas recipients.

We agree that entities that collect personal information from individuals have certain responsibilities for the security of that information when they provide it to overseas recipients. However, we think that section 20, which deems an entity to be liable for the acts of overseas recipients of personal information, is unduly broad. Even if an entity takes all reasonable steps to ensure that the overseas recipients to which they disclose personal information will comply with the APPs, there remains a possibility that the overseas recipient may not comply, which the Australian entity cannot prevent.

We would recommend that rather than deemed liability for the acts of overseas recipients, section 20 should impose an obligation on an entity to use reasonable endeavours to ensure that the overseas recipient remedies any act or omission that would otherwise constitute a breach of the APPs. This would act as an incentive for entities to ensure that the overseas recipients they deal with comply with the APPs.

* * *

We are grateful for the opportunity to provide our thoughts on the exposure draft and would be pleased to participate further in any discussions to be held on the proposed legislation.

We look forward to reviewing the proposed companion legislation containing the associated administrative functions and enforcement powers. The impact of the proposed APPs cannot be considered fully until they are reviewed in that context.

Telstra Corporation Limited

10 August 2010

To contact us:

Helen Lewin – Chief Privacy Officer – helen.lewin@team.telstra.com