Australian
Privacy
Foundation

http://www.privacy.org.au
Secretary@privacy.org.au
http://www.privacy.org.au/About/Contacts.html

Ms Joanna Hamilton
Executive Officer
Services Trade and Negotiations Section
Goods and Investment Branch
Department of Foreign Affairs and Trade
tpp@dfat.gov.au.

7 September 2012

Dear Ms Hamilton

Re: Submission on the Protection of Privacy and Personal Data in Relation to Free Trade Agreements

The Australian Privacy Foundation (APF) considers it is essential to protect the privacy of Australians in all provisions of Free Trade Agreements (FTAs), including the proposed Trans-Pacific Partnership Agreement (TPPA). The protection of privacy and personal information are fundamental human rights and must be adequately protected in any trade agreements that deal with data processing.

In particular the APF is concerned with the increasing pressure from organisations located or undertaking business in Australia to exchange, store and process data in other jurisdictions, including those where Australian laws or adequate, equivalent legal protection do not apply. In this context, we are especially alarmed with the increasing trend for personal data to be stored and processed in the 'cloud' without sufficient privacy safeguards. The APF considers that the current Australian laws (including proposed law reforms) are inadequate in important respects, and must be urgently strengthened.

The APF notes the increasing pressure from other countries to include data (both defined as a 'service' or a 'product') within FTAs. The privacy and personal data of Australians are of legitimate public interest and must be adequately protected.

The attached submission addresses:

1. Specific requirements to be included in a definition of personal data that takes into account existing and emerging practices and technologies
2. Inadequacy of protection for personal data set out in existing and proposed Australian privacy legislation
3. Cross Border Privacy Rules
4. Jurisdictional issues.

We acknowledge the broad scope of this submission, but believe the additional information provided is required to explain our concerns, justify our approach and provide sufficient background material for negotiators.

In summary, we submit that, 'personal data' defined as any 'data that enables a person to be identified either directly, or after integration or linkage with other data' should be expressly excluded from the provisions of all and any FTAs, including the proposed TPAA.

We submit that, in the absence of satisfactory international instruments or arrangements that adequately protect data privacy, the exclusion of personal data from the scope of FTAs is the only effective way of protecting the fundamental human rights to privacy and data protection. In making this recommendation, we note that this would not affect the transfer of personal data under existing Australian information privacy laws, but that it would prevent the erosion of privacy through agreements that are directed at the promotion of free trade, and not at the protection of privacy.

Finally, we note that this submission will be published on your website.

Yours sincerely

Dr Julie Cameron
Board Member
Australian Privacy Foundation

Australian Privacy Foundation
Submission to the Department of Foreign Affairs and Trade
Office of Trade Negotiations

7 September 2012

Protection of Privacy and Personal Data in Relation to Free Trade Agreements

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The APF aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defense of the right of individuals to control their personal information and to be free of excessive intrusions. For further information about the APF please see Appendix A

The APF uses the Australian Privacy Charter published in December 1994 as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Privacy Charter, please refer to www.privacy.org.au/About/PrivacyCharter.html.

The APF is committed to the protection of privacy and personal data as fundamental human rights. Hence, we are concerned with threats to the privacy and personal data of Australians that may be posed by Free Trade Agreements (FTAs) which Australia may become a party to, including the proposed Trans-Pacific Partnership Agreement (TPPA). The protection of privacy and personal data is fundamental to the promotion of trust online, and is therefore an essential pre-requisite to the development of e-commerce. We note that the importance of the protection of personal data has been recognised, albeit very imperfectly, by the incorporation of online data protection provisions in the e-commerce chapters of bilateral FTAs to which Australia is a party.

Given the potential for FTAs to undermine the protection of privacy and personal data by liberalising the processing of personal data, including the trans-border processing of personal data, this submission focuses on four significant issues that must be taken into account in any negotiations, namely the:

- Definition of personal data in the context of FTAs
- Inadequate protection of personal data under existing Australian law
- Need for adequate and enforceable cross-border privacy rules
- Need for jurisdictional transparency.

Definition of Personal Data in the Context of Free Trade Agreements

The APF believes that people have fundamental rights to the privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person) and freedom from surveillance (Australian Privacy Charter, December 1994). As information privacy is concerned with the protection of personal data (or personal information), the definition of 'personal data' is essential to the protection of this aspect of privacy.

Personal data is information about an identified person or identifiable person, no matter in what format it occurs (eg. sound, image, data, biometrics). This means that personal data is not restricted to obviously identifying information – such as the name, address, date of birth, sex, nationality or religion of a person – but extends to all information, or combinations of information, from which an individual may be identified. Emerging organisational practices involving techniques like data integration for risk and lifestyle profiling, combined with the use of electronic tracking and surveillance, increase the potential for formerly anonymous information to be accessed and combined in new ways which identify individuals. Consequently, these practices require an expanded definition of 'personal data'. For example, now that digital devices can be linked to a

person by organisations that collect personal information, the IP (internet protocol) address from which services and content are accessed should, in some circumstances, be considered 'personal data'.

The APF is concerned that apparently 'de-identified' data, when aggregated with data from numerous sources, which can now readily occur, can no longer adequately protect privacy. Data collection has now become so ubiquitous and abundant, that removing names and unique identifiers and aggregating groups cannot prevent re-identification. This is particularly true when collecting data about small groups of people with minority characteristics. For example, it would not be difficult to re-identify an Iranian medical practitioner in a rural town, or a woman carpenter in Sydney. We therefore argue that, at the least, sensitive de-identified information (including health data) should be included in any definition of 'personal data'.

Converging technologies mean that the personal data can be defined as a 'service' or a 'product'. For example, 'broadcasting' and audiovisual services can be provided either by traditional transmission methods or via the internet and 'downloaded' or 'streamed'. Personal data can also be included within 'content'. There is ambiguity as to whether search engines provide a 'service' or are a 'product'. Some search engines can return 'personal data' without the knowledge of the 'owner' or 'custodian' of the data if personal computers are not adequately protected from 'web crawlers'.

Given the emergence of practices that increasingly enable the identification of individuals from information that was previously either anonymous or de-identified, we submit that an adequate information privacy regime must be based on a definition of 'personal data' that includes any data that enables a person to be identified either directly, or after integration or linking with other data.

We submit that 'personal data' be defined as any 'data that enables a person to be identified either directly, or after integration or linkage with other data'

Exclusion of Personal Data from Free Trade Agreements

The APF observes increasing pressure from organisations, located or undertaking business in Australia to exchange, store and process data in other countries, in the 'cloud' and in other jurisdictions. We note the increasing pressure from other countries to include data (both defined as a 'service' or a 'product') within FTAs. The privacy and personal data of Australians are of legitimate public interest and must be adequately protected.

The APF is very concerned about the numerous breaches of privacy and misuse of personal data both in Australia and overseas. While personal data may have business value if exploited, it is not primarily a business asset. It is a potentially high risk, non-revocable information set, tied to and capable of profoundly harming individuals. Normally when data is sent overseas, the individuals who are the data subjects are not a party to the contracts under which their details are sent offshore. Therefore, they are unable to exercise any of the normal restraints on information misuse that may occur. In most business agreements and contracts, both the exporting and importing party aim to minimise their own liability and exposure to any claims of misuse of personal data or breaches of privacy by individuals who are the data subjects.

The lack of a Free Trade Agreement does not prevent Australian organisations engaging in e-commerce or other commercial transactions which may include the transfer of less sensitive personal data, provided they enter into legally binding bilateral agreements with partners that explicitly and adequately protect personal data and privacy. These agreements and contracts must provide provisions that facilitate claims against misuse of personal data or breaches of privacy that are enforceable by individual Australians.

The APF believes in the principle that individuals should give 'informed consent' prior to their personal data being transferred outside Australian jurisdiction by organisations for collection,

storage or processing. Such consent must not be bundled with consent given to other matters. We acknowledge that individuals may choice to provide personal data to organisations operating outside Australia. This is a personal decision, presumably based on 'informed consent'. However, cross-border flows of personal data by organisations should not be permitted to over-ride individual concerns.

The APF believes in the principle that cross-border flow of personal information should be restricted to protect personal information. Exclusion of personal data is not a 'restrictive' policy or practice. Australians, as individuals and organisations, have sufficient experience with the misuse of personal data to understand the significant risks to privacy that arise from inadequate protection. We strongly believe Australia must retain the right to require on-line service providers (particularly those involved with personal data) to locate physical infrastructure and undertake storage and processing within our borders. We note that health data is considered so sensitive and the risks to privacy so high that it is forbidden to transfer of this form of personal information outside Australia.

We submit that 'personal data' should be expressly excluded from the provisions of Free Trade Agreements.

The following sections address key reasons for this conclusion, namely the:

1. Inadequacy of protection for personal data set out in existing and proposed Australian privacy legislation
2. Need for adequate and enforceable Cross-Border Privacy Rules
3. Jurisdictional issues.

We believe this information is required to explain our concerns, justify our approach and is important background material for negotiators.

1. Inadequate Protection of Privacy and Personal Data in Australian Legislation

The exclusion of personal data from FTAs is currently even more important than previously because of the inadequate protection of privacy and personal data provided by Australian legislation.

The APF is concerned that the current Privacy Act 1988 and amendments does not adequately protect personal data, particularly in the context of cross-border (or trans-border) disclosure. The National Privacy Principle (NPP) 9 – Trans-border data flows limits the right of "an organisation in Australia or an external Territory" to transfer "personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country" if principles for handling information are substantially similar to the NPPs, or with an individual's consent, request etc. and the organisation has taken "reasonable" steps to ensure the information will not be "held, used or disclosed by the recipient…inconsistently with the NPPs". The apparent protection afforded by this legislation has been undermined by offshore collection of personal information (eg. through the use of call centers) and integration of data from multiple sources.

There are too many exceptions in the legislation. For example, the Privacy Act 1988 does not apply to small business. Now that information and communications technologies are ubiquitous and extremely powerful, small business can use these technologies in the same way and on a similar scale to larger businesses and organisations that must adhere to the Act. For example, the amount of storage available (including in the 'cloud') enables large amounts of personal data to be stored and processed cheaply and quickly by small organisations and even individuals.

'Cloud computing' raises complex issues and uncertainty in relation to jurisdiction. The use of 'cloud computing', where the location of data is ambiguous and certainly not transparent to the data subjects, exacerbates the inadequacy of protection. This lack of clarity also relates to control and accountability. This situation is not adequately addressed in current privacy legislation.

The APF has opposed breaches of privacy and exploitation and misuse of personal data (eg. by Google). However, there appears to be little chance of breaches that are exposed, being

appropriately addressed under the current Australian legislative regime and no evidence of effective remedy or compensation.

The APF is even more concerned about the proposed changes to the Privacy Act 1988 currently being considered. The APF Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs, which details our concerns, is published as Submission Number 030 (please refer to www.privacy.org.au). Relevant extracts are set out as Appendix B to this submission.

We argue that the Australian Privacy 8 (APP 8) on cross-border disclosure provides no real protection. The accountability is fictional. There is, for example, no requirement to inform individuals that their personal data is being sent outside Australia or where it is being sent. Specifically we recommend (see pages 19-20):

"Submission 47: The solution to the problems of APP 8 is to delete the words 'the entity reasonably believes that', so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal.

Submission 49: The exceptions for international agreements should be deleted, as they will encourage policy laundering.

Submission 50: The two key changes required to APP 8 are: (i) an objective standard for the level of privacy protection provided in another country; and (ii) more disclosure of the details of an overseas transfer to individuals before they are asked to consent to it (and thus lose their rights to any remedy)."

2. Need for adequate and enforceable Cross-Border Privacy Rules

Privacy is a global issue. Confidence in the security of personal data is a prerequisite for ecommerce. Australians need to trust their personal data will be treated appropriately when sent offshore. Other countries need to trust Australia will deal appropriately with the personal data of their citizens. Global, objective standards need to be in place that are transparent and provide certainty.

The APF notes Professor Graham Greenleaf's finding confirming the growing importance of the OECD's privacy guidelines, the Council of Europe Data Protection Convention and European Union Privacy Directives ("Overview of the Global Trajectory of Data Privacy Laws" published in *Privacy Laws & Business Asia-Pacific Compilation*, December 2011). Currently Australia does not provide adequate privacy protection to receive 'favourable Opinions' from the Article 29 Working Party. If Australia intends to provide an 'adequate' level of protection of privacy to enable the free flow of information from the European Union countries and others that comply with their terms and conditions, any Cross-Border Privacy provisions within Free Trade Treaties should aim to incorporate these requirements as a minimum standard. This would assist Australian organisations and enhance their opportunity for trade and e-commerce.

The APF notes the endorsement of the Cross-Border Privacy Rules system endorsed by the APEC Electronic Commerce Steering Committee Group in September 2011 (refer to "APEC CBRP – Ready to Party but Will Anyone Come?" (Nigel Waters published in *Privacy Laws & Business Asia-Pacific Compilation*, December 2011). However, it remains uncertain if countries will provide resourcing or be willing to establish Accountability Agents. The APF also questions whether countries that do not comply with the rules will be excluded. We are concerned that the business case for organisations to seek certification under this system is not clear.

3. Jurisdictional Issues

The APF believes in the principle of transparency of jurisdiction, laws, regulations, procedures and administrative rulings concerning the treatment of personal data. A major concern is that whenever data is sent outside Australia, jurisdictional transparency is diminished or lost. For example, even if an individual discovers a breach has occurred, how does an Australian individual seek remedy? If an individual is able to seek remedy, the costs and complexity of taking action in courts outside Australia is prohibitive.

We believe in the principle that regulatory authorities need to be independent and accessible to individuals. They need to be able to provide equitable remedy for breaches of the privacy of individual Australians by organisations responsible for protecting personal data, regardless of the location in which the breach occurred.

Jurisdictional issues are even more complex now that organisations are using 'cloud computing' and storing data in the 'cloud'. More than one jurisdiction may apply to a data set at different times according to who owns the data, who processes it and where it is physically stored at a particular time. The 'cloud' can be compared to the 'high seas' but unlike the 'high seas' no body of law and jurisdiction has yet been developed.

Increasingly both local consumers, business and government 'cloud' customers are seeking to introduce data sovereignty clauses and concepts into arrangements in reaction to the emerging realization of the previously poorly appreciated but potentially severe risks in hosting data in jurisdictions outside the easy reach of local contractual and regulatory remedies. This trend is exacerbated because global scale providers are often unwilling to negotiate on terms and liability. Privacy and personal information security are key considerations for 'jurisdiction aware hosting'. It is critical that nothing in any ostensible FTA constrains this sensible trend. There is a potential for commercial conflict between local cloud business providers and purchasers seeking to implement an approach that creates an 'Australian cloud' and offshore businesses that may argue the sovereignty clauses are improper for trade purposes and/or under FTAs. It is important that foreign commercial interests are not elevated over domestic data sovereignty and expectations of information security.

There is increasing vagueness of what the term 'carrying out business in Australia' means in practical terms for privacy and data protection. Organisations like Facebook and Google may operate within Australia but claim to be subject to laws in the USA. We need to retain the right to require organisations to 'operate' locally in accordance with Australian legislation.

Conclusion

The APF supports the need to promote international trade and commerce. Some of our members have been involved in establishing international ebusiness solutions and negotiating contracts among nominated trading partners located in Australia and overseas. However, the protection provided in bilateral agreements and the controls required when cross-border data flow involves commercial and trade data, are very different to the provisions and protection provided and the controls required if personal data is involved. The APF does not consider the provisions and protection that currently could be included in a Free Trade Agreement can adequately protect the personal data and privacy of Australians.

Appendix A
Australian Privacy Foundation: Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law. For information about current Board Members please refer to http://www.privacy.org.au/About/Contacts.html/

The Board is supported by our patrons, The Hon. Michael Kirby AC CMG and The Hon. Elizabeth Evatt AC and an Advisory Panel of eminent citizens, including a former Prime Minister. A full list of the panel is available at http://privacy.org.au/About/AdvisoryPanel.html.

The following pages provide access to information about the APF:
• Policies http://www.privacy.org.au/Papers/
• Resources http://www.privacy.org.au/Resources/
• Media http://www.privacy.org.au/Media/

The following pages provide outlines of several campaigns the APF has conducted:
• The Australia Card (1985-87)
http://www.privacy.org.au/About/Formation.html
• CreditReporting (1988-90)
http://www.privacy.org.au/Campaigns/CreditRpting/
• The Access Card (2006-07)
http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
• The Media (2007-)
http://www.privacy.org.au/Campaigns/Media/

Appendix B
Extract from the Australia Privacy Foundation's Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs Privacy Amendment (Enhancing Privacy Protection) Bill 2012, August 2012
Published as Submission 030.

Overview of the APPs
The proposed Australian Privacy Principles (APPs) are weaker than the ALRC's proposed UPPs and the current IPPs and NPPs, and unless significantly improved during the Parliamentary process will lead to an overall reduction in privacy protection. Regrettably, the government has gone backwards instead of forwards in terms of modernising the principles, and seems to have been unduly influenced by both business and agency interests, to the detriment of the interests of the citizens and consumers that the Privacy Act is intended to protect. In the case of government agencies, a raft of changes have been 'slipped in' at the last minute to avoid some agencies having to rigorously apply well-designed existing exceptions. Such lazy drafting and special pleading should be rejected. There are a few improvements to the ALRC proposals in the government's Bill, but in many cases proposed changes to the language of the principles which appear minor and superficially innocuous in fact have very significant adverse effects. In particular, the cross-border disclosure principle, which has an ever increasing importance in the context of borderless networks and 'cloud' computing, is seriously inadequate.

APP 8: Cross-border disclosure – Fictional accountability, no real protection
The most controversial new principle is APP 8, which, at the urgings of the ALRC, abandons what it calls a 'border protection' approach in favour of the approach misdescribed as 'accountability'. Given that the existing NPP 9 in effect allows personal data to be exported to any country (not matter how weak its laws) if 'reasonable steps' are taken to ensure that the data is used consistently with the NPPs, and that Australian law has not developed any interpretation of what are 'reasonable steps', the differences in the Australian context are probably more apparent that real. The real issue is whether what is proposed is any better than the current extremely weak protection.

Under APP 8.1, an Australian company or agency will be able to send personal information anywhere in the world (subject to APP 6). If it is not completely exempt from any liability for what then happens to the information (under nine separate exemptions), then it will be liable under the Australian Act for any acts by the overseas recipient that would breach the APPs if the APPs applied to it (s20). This applies to acts by any overseas recipient, even one that might be exempt under Australian law in Australia (for example, a 'small business'). The Australian exporter will also breach APP 8 if it fails to take reasonable steps, before exporting data, to ensure that the overseas recipient does not breach the APPs (other than APP 1). There is no definition of such steps, nor any proposed power for the Commissioner to issue guidelines or model contracts. We submit that it is essential that the Commissioner should issue guidelines concerning model clauses or a model contract clauses before any organisation can rely on a contract as meeting the 'reasonable steps' test in APP 8.1.

Curiously, the exporter does not have to take steps to ensure the importer complies with APP 1, the only APP where it is relatively easy to prove that an overseas recipient is in breach (because it does not have an available Privacy Policy). And that indicates the main weakness: in relation to all the other APPs, how does an individual in Australia prove on the balance of probabilities how a breach has occurred in an overseas country, and one which by definition has no similar privacy laws of its own (if it did, the exporter would be exempt from any liability under one of the exemptions)? The purported 'accountability' remains a fiction. We submit that a breach by an overseas recipient should be a rebuttable presumption if damage to the individual can reasonably be assumed to have resulted from the export. That would be real 'accountability', but it is lacking at present. We have amended s20 to this effect, by addition of s20(3) to provide some reasonable

prospect for complainants to enforce 'accountability' without facing insurmountable problems of onus and burden of proof.

Another weakness is that APP 8 won't even require individuals to be given notice at the time that their data is going … somewhere or other. If organisations were required to give such notice, they would think twice before doing so, and individuals would be on guard for damage. We have already commented above on the weakness in APPs 1 & 5 that only require policies and collection notices to specify likely destination countries 'if practicable' and contain no requirement to explain the level (or lack of) privacy protection in those countries. But APP 8.1 is at least an attempt at regulation of overseas transfers. It is however fatally undermined by APP 8.2, coupled with s16A, which provides at least nine separate grounds on which a data exporter can be exempt from even the theoretical liability/'accountability' of APP 8.1. The first exception is where the exporter 'reasonably believes' in the existence of an overseas law or binding scheme, that 'has the effect of protecting the information in a way that, overall, is at least substantially similar' to the APPs, with mechanisms for redress and enforcement (APP 8.2(a)). As we have emphasised in previous submissions, this is completely unacceptable basis for allowing cross border transfers. Some organisations will inevitably make self-serving judgements about the level of protection in other jurisdictions and/or pay for advice that supports their desire to transfer. Similar protection should be an exception to any prohibition on transfer, but it must be based on objective criteria.

The only practical approach to remedying this defect in the current Bill is simply to delete 'the entity reasonably believes that', so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal. Such ex post facto determinations may discourage exports of Australians' personal information to countries where privacy protection is questionable, but that would be a good result. It would be preferably if there could be some prior considered assessment of similarity or adequacy by experts, such as the Privacy Commissioner, and this could be achieved by guidelines under the current Act. A binding 'white list' scheme is a feature of privacy laws in some other jurisdictions and could usefully be adopted in Australian law, provided it was based on objective assessments, not politics.

Submission 47: The solution to the problems of APP 8 is to delete the words 'the entity reasonably believes that', so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal.

The second exception is where there is consent based on explicit notice that the exporter accepts no liability ('accountability') for whatever happens overseas (APP 8.2(b)). But there is no requirement for the organisation to explain the 'risk' either generally or in relation to the specific destination, and consent can still be 'implied' so this is likely to result in completely ineffective 'small print' notices tucked away in standard terms and conditions.

Submission 48: Any exception based on explicit notice that the exporter accepts no liability must include an express requirement for the organisation to explain the risk involved.

Another exception is where Australia is a party to some international agreement that relates to information sharing (APP 8.2(e)) – this would in effect abrogate Australian sovereignty and is an example of 'policy laundering' – hiding behind often spurious claims of 'international obligations' to justify actions which would not otherwise be lawful.

Submission 49: The exceptions for international agreements should be deleted as they will encourage policy laundering.

Although we reject the abandonment of a 'border control' approach that underlies APP 8, the existing NPP 9 is itself so weak that an improved APP 8 could be an improvement. It is not an

improvement in its current form, but with the changes we propose, it would be an improvement on NPP 9.

Submission 50: The two key changes required to APP 8 are: (i) an objective standard for the level of privacy protection provided in another country; and (ii) more disclosure of the details of an overseas transfer to individuals before they are asked to consent to it (and thus lose their rights to any remedy).