Friday 20 July 2012

Committee Secretary
House Standing Committee on Social Policy and Legal Affairs
By email: committee.reps@aph.gov.au

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

This submission is made on behalf of Facebook, Google, IAB Australia and Yahoo!7 (the "Submitters"). We take great pleasure in the opportunity to provide our collective feedback to the Committee with respect to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 ("Proposed Law") currently before Parliament.

Each of our organisations either operates or represents operators in the digital sphere and all are strongly committed to privacy. Our success is tied to ensuring that people have positive experiences on the platforms we provide and fundamental to this is securing and maintaining users' trust – which is key to success as an online service provider. Ultimately, it is imperative to a provider's bottom line to get users' privacy and security right. Otherwise, users will switch to a different service. This is most true in the highly competitive world of the web, where an alternative is just a click away.

Our shared commitment to privacy squarely aligns with the proposed new Australian Privacy Principle 1 that requires entities to manage personal information in an open and transparent way. Each of the Submitters promotes privacy through clearly notified privacy policies and a variety of additional tools including privacy setting controls, interactive controls and general education and awareness activities. Please refer to the Appendix for more information about each of the Submitters.

Together, we provide global communications services that allow many millions of Australians to connect and enjoy valuable services. The platforms that we provide also support Australia's innovators and entrepreneurs to generate new revenue streams and reach new audiences.

The Australian Government recognised the tremendous benefit that global networks can deliver for the Australian economy and society when it set as its goal that Australia become a world leading digital economy by 2020 in the *National Digital Economy Strategy*.[1] The very nature of digital economy services that can contribute to this goal is such that they will operate across borders. Consequently, to become a global leading digital economy by 2020, the Australian Government must ensure that its privacy laws provide business certainty and permit innovative, global digital economy services.

Each of the companies making this submission, with the exception of IAB Australia, provides online services globally and we note that Australian privacy law is one of many national regulations impacting the online services industry. Companies that operate globally must adopt policies that govern their services generally and that permit data to be used across those

[1] http://www.nbn.gov.au/the-vision/digitaleconomystrategy/

services – not just in one of the many countries in which they operate. Organisations who operate across multiple countries adopt different approaches to compliance with these national laws; some choose to apply one overarching privacy policy globally which sits over and above what the law requires of them in any one jurisdiction, whilst others take a market by market approach. The reality and ubiquity of cross border data transfers, even for companies who are solely based in Australia but who chose to process or store data offshore or who operate Australian-based digital economy businesses, needs to be treated in a non-discriminatory manner within the Proposed Law and the Australian Privacy Principles. We will draw attention to some more specific issues relating to the interaction of different privacy laws and cross border data transfers within this submission.

Detailed Comments on the Proposed Law

We have seven specific comments on aspects of the Proposed Law that may have unexpectedly negative consequences for consumers and Australia's digital economy.

1. APP2 - anonymity and pseudonymity

The newly formulated APP 2 recognises the importance of the right of anonymity and pseudonymity in privacy, as well as legitimate exceptions. All have a role to play in the digital economy and consequently, it is important that the rights and exceptions are clearly and consistently expressed.

At present, however, there appears to be a drafting error in APP2.

APP2.2(b) currently states: "it is impracticable for the APP entity to deal with individuals who have not identified themselves." This drafting error is repeated in the Explanatory Memorandum, which refers "the nature of a business or a service provided by an organisation [that] is not compatible with providing the option to interact anonymously".

We believe that APP2.2(b) should reflect both anonymity and pseudonymity, as outlined in APP2.1.

As such APP2.2(b) should be amended to read: "it is impracticable for the APP entity to deal with individuals who have not identified themselves or who use a pseudonym". Similarly the Explanatory Memorandum should be amended as follows:

> "There may also be circumstances where the nature of a business and the service provided by an organisation is not compatible with providing the option to interact anonymously or pseudonymously."

We also believe it would be helpful for the Explanatory Memorandum to clarify that whether it is impracticable to enable anonymous or pseudonymous use is something that must be considered on a case by case basis and will depend on the context. It would also be helpful to clarify that such use is impracticable:

a) for opt-in services that rely on a real name culture as an essential part of their service, for example, to help people find and connect with each other and to promote user safety and security. An example of this is Facebook. In their recent audit of Facebook the Irish Data Protection Commissioner confirmed that requiring real names and identities was necessary for child protection and related safety reasons;[2] and,

b) for organisations operating ecommerce websites where there is a need for users to authenticate their identity through the use of credit cards.

2. APP3 – collection

APP3 is focused on collection and the Explanatory Memorandum provides an expansive explanation of what amounts to a "collection" under the proposed privacy laws, including under paragraph 5B(3)(c). It is important that appropriate geographical nexus provisions apply to national privacy laws so that international internet services can be supplied with reasonable clarity as to the laws applicable to those services and in particular the rules governing collection, use and disclosure of personal information by organisations carrying on business in particular jurisdictions. If an appropriate geographic nexus is not a feature of national privacy laws, this sets a precedent for other countries to adopt legislation that may have uncertain or inappropriate extraterritorial effect on Australian companies.

The Explanatory Memorandum explains that the Government intends that an extra-territorial link is established when information is collected from an individual who is physically located in Australia even if there are no other nexus points with Australia. We suggest that this should be further clarified to ensure that the intended scope of operation of the Act is clear and workable in practice.

Where information is collected in the course of operation of an overseas internet site by an organisation which does not conduct business in Australia, it is appropriate that the activities of that organization are regulated by the jurisdictions in which that organisation conducts business and that the organisation is not subject to double jeopardy or conflicting laws. There is room for further clarity in the Explanatory Memorandum so that it is clear that information is collected at the place of the service provider collecting the information, not the place where the user is or may be presumed to be at the time the information is collected. In any event, a service provider collecting the information often will not be in a position to know where the user is at the time that that information is collected. For example a user may be transacting anonymously or roaming from the user's location. An IP address or other transaction data may not be sufficient to enable the internet service provider to identify the location of the user. For clarity, the Proposed Law should state that an organisation collects personal information where the information is collated, processed or stored.

---

[2] See page 137 http://dataprotection.ie/viewdoc.asp?DocID=1182 ("[W]e consider that FB-I has advanced a sufficient rationale for child protection and other reasons for this policy position and do not consider that from an Irish data protection law perspective that there is sufficient justification as to require that FB-I adopt a different policy.")

Yahoo!7 has an alternative view on this particular issue which it will provide in a separate submission.

3. APP7 – direct marketing

We appreciate that the Government wishes to provide clarity around the circumstances in which direct marketing is permissible and how people can be empowered to control their experience in relation to the direct marketing messages they receive. However, we are concerned that, at present, the proposed description of "direct marketing" in the Explanatory Memorandum would prima facie prohibit all forms of promotional communications between businesses and consumers and would potentially undermine ad-supported business models.

At present, the Explanatory Memorandum states:

> Direct marketing involves communicating directly with a consumer to promote the sale of goods and services to the consumer.

This is so broad as to potentially cover all forms of communications between businesses and consumers that include any promotional material, including, for example, free-to-air television advertisements and free online, ad-supported services such as those offered by the Submitters.

The Explanatory Memorandum then continues to provide examples that are illustrative and primarily focus on the means of communication and the origins of the data used to contact consumers.

> The direct marketing communication could be delivered by a range of methods including mail, telephone, email or SMS. Direct marketers compile lists of consumers and their contact details from a wide variety of sources, including public records, the white pages, the electoral roll, registers of births, deaths and marriages and land title registers. They also include membership lists of business, professional and trade organisations, survey returns and mail order purchases.

However, these illustrative lists do not provide clarity around what type of communication is considered to be direct marketing, and which is not. Our understanding is that direct marketing is typically understood to refer to, in addition to the characteristics described in the secondary materials, communications that are primarily promotional in nature and that are unsolicited. We also understand that the purpose of the legislation is to apply to the actual provider of a purely and unsolicited marketing message, and not a platform that may be used to provide that missive.

If a specific definition is preferred, a useful model may be:

Definition of direct marketing

"*direct marketing*" means an organisation promoting the availability of or offering goods or services by an unsolicited communication by mail, telephone, electronic mail or electronic messaging or like electronic communications that is initiated by an organisation and addressed to an individual, but does not include:

a) *an organisation promoting the availability of or offering goods or services in response to the request, query or other communication initiated by an individual;*

b) *a communication reasonably related to:*

- *an ongoing service or customer relationship between an individual and the organisation;*
- *a transaction or transactions conducted between an individual and the organisation;*
- *a transaction that the organisation has reasonable grounds to consider the individual has manifested an interest in conducting with the organisation;*

c) *a communication that a consumer has consented to receive. Consent may be express or consent that is reasonably inferred from the conduct or the business or other relationships of the individual or organisation concerned;*

d) *a communication of a kind specified in the regulations or required by law; or,*

e) *a communication that is addressed to one individual or group of individuals at the direction of another individual,*

and "direct marketing communication" has a similar meaning."

Use of personal information for the purpose of direct marketing

Personal information is not used for the purpose of direct marketing if the only use of that personal information is inherent in the identifier for the addressee, such as an email address or like identifier of the intended recipient of an electronic communication, or the address for physical delivery of physical mail, provided that such email address or like identifier or address for physical delivery was not obtained from any source other than the organisation or its related bodies.

Clarification

If a communication is regulated as a commercial electronic message pursuant to the *Spam Act 2003* but permitted to be made in accordance with the *Spam Act 2003*, this principle does not apply to the extent that the commercial electronic message is communicated in accordance with the *Spam Act 2003*.

In our view, the Proposed Law should not be read to (and we believe it is not intended to) permit a consumer to opt out of all direct marketing, if receiving direct marketing is part of the value

exchange of the service that the consumer is choosing to receive. To avoid this ambiguity, APP7.2 and APP7.3 should be rephrased. APP7.2 and APP7.3 each require that an opt-out of direct marketing be provided. However it is not clear that the opt-out be from receipt of direct marketing *that relies on personal information*. Rather it is written as an opt-out of direct marketing altogether. In the event that 'direct marketing' were interpreted to include advertisements, this would undermine advertising based business models, which is surely not the intention of the Proposed Law.

We would like APP7.2 and APP7.3 to require an opt-out of direct marketing *that relies on personal information*. This will allow advertisements to still be served (not based on personal information). This is particularly important where the advertisements are part of a service that is free to access and ad-supported.

4. APP8 – cross border data flows

The Internet has become an unparalleled engine for innovation, economic growth and social discourse, it is a medium that enables global communication and collaboration. It is important for Australia's economic interests to ensure the global internet remains open as the essential information infrastructure of tomorrow. Trade is vital for Australia and services constitute an increasingly important part of the economy. The Department of Foreign Affairs and Trade expresses this reality well:

> *Australia is a world-class provider of a range of services, such as telecommunications, travel, banking and insurance. Services exports play a significant role in our economy and represents about 70 per cent of Australia's gross domestic product (GDP) and employ four out of five Australians.*
>
> *Services also play an increasingly important role in our international trade, with services exports growing by an average of 6.5 per cent per annum between 2005 and 2010. In 2010, total trade in services accounted for 19.6 per cent of Australia's total trade in goods and services.*[3]

In the digital age, the ability to export services is dependent upon the ability for information to flow across borders. In a global digital economy, foreign-based and locally based companies will frequently engage in cross-border disclosures of information and most international agreements and international fora acknowledge that this is an important component of economic activity. As such, privacy law must support cross-border data flows whilst imposing accountability. We recognise the need to impose a requirement that organisations be accountable for the information that they share across borders. However the current drafting of this provision places digital economy organisations at inappropriate jeopardy, as set out below.

We wholeheartedly support requiring disclosing entities to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. However, we are concerned that an entity disclosing personal information about an individual to an

[3] http://www.dfat.gov.au/trade/negotiations/services/overview_trade_in_services.html

overseas recipient is subject to strict liability (by virtue of section 16C(2) (Acts and practices of overseas recipients of personal information)) even if that entity took all reasonable steps to ensure that the overseas recipient complies with the APPs.

An APP entity disclosing personal information about an individual to an overseas recipient, that discharges an onus of establishing that it took all reasonable steps to ensure that the overseas recipient complies with the APPs, should thereby make out a defence to liability pursuant to APP8.1.

We note that Section 16C, which outlines the strict liability, purports to adopt an OECD and APEC sanctioned accountability principle. However APP8 and Section 16C go far beyond the tailored approaches taken by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[4] and the APEC Privacy Framework of 2004[5]. Recognising the variation in specific national data protection rules, both the OECD and APEC frameworks avoid overly-prescriptive rules. For instance, the APEC Privacy Framework provides in Principle 9 – Accountability:

> A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Specifically, the OECD principle foresees a due diligence requirement, and not a strict liability model. Similarly, the OECD Guidelines are broadly framed, stating specifically:

> Paragraph 14: Accountability Principle
> 62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

---

[4] http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html
[5] https://www.google.com/url?q=http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx&sa=U&ei=HbzFT4jVLKrD2QWz8vm9AQ&ved=0CAUQFjAA&client=internal-uds-cse&usg=AFQjCNFHJEcagBOygdhCLzIofkAv1HwDsg

Again, it does not require the specific structure adopted by the proposed APP8.

Continuing in the vein of cross-border data flows, we believe that the drafting in APP8.2(a) does not have the intended effect. We understand that the intention is for APP8.2(a) to enable transfer of data to economies that are participating in the APEC Privacy Pathfinder, and in particular the Cross Border Privacy Enforcement Arrangement (CBPEA). As presently drafted, APP8.2(a)(ii) does not clearly include the ability of individuals to take action through the CBPEA - that is, that they would be able to contact their local privacy authority (eg the Australian Privacy Commissioner) who could then pursue a matter of cross-border data flows under the CBPEA with their relevant counterpart (eg the US Federal Trade Commission). We would like to highlight the importance in this section of focussing on actionable and meaningful recourse being available to users who wish to take action through the CBPEA. We therefore request that APP8.2(a)(ii) should be clarified to give full effect to the APEC Privacy Pathfinder and the CBPEA.

In addition, there may be other arrangements between regulators that allow Australians to pursue privacy concerns with overseas entities. Therefore, the clarification described above should not be confined to CBPEA but should allow for any current and future arrangements between regulators.

5. <u>APP Code related provisions Schedule 3</u>

APP Codes, once registered, acquire quasi-legislative status in that a breach of a registered APP code is an interference with the privacy of an individual.

We endorse the development and use of APP Codes and the safeguard of review before registration by the Commissioner. However any APP entity may propose a code that may, once registered, bind a specified class of APP entities, whether or not the APP entity is a body representative of the APP entities to be bound and whether or not those entities were involved in the code development process or consulted as to any draft code. It is important to ensure the participation of any entity that will be bound by an APP Code in the adoption and implementation of that code.

Section 26F at page 145 states that the APP entity or APP entities that develop a code make a draft of that code publicly available, invite submissions, allow at least 28 days to run for submissions to be made, and give consideration to submissions made within the specified period. There is no requirement that the APP code developer represents, or consults a representative sample, of those APP entities that would be subject to the code. Nor is there a requirement for the code developer to actively publicise the availability of the draft code for submissions or inform the Commissioner as to the nature and effect of any submissions received.

Although we understand that the Commissioner may make guidelines (Section 26V, page 154) as to good practice in code development that might address some or all of the concerns raised

above, we suggest that it would be appropriate for the Bill itself to include some basic safeguards as to code development. We contrast, for example, clause 85 in Schedule 7 to the Broadcasting Services Act 1992 and section117 of the Telecommunications Act 1997.

We suggest that the provisions should at the minimum:

- require the APP code developer to demonstrate to the Commissioner that the APP code developer directly represents all of the APP entities proposed to be to be governed by the Code or that the APP code developer has consulted broadly within that class or group;
- require the APP code developer to take active steps to publicise that the draft code has been released for submissions and to solicit submissions;
- require that submissions must be accepted by a convenient mechanism for making submissions, such as internet lodgement;
- require that any draft code (as revised after consideration is given to submissions) when lodged for registration is accompanied by a document that fairly summarises the range, nature and content of written submissions received or includes all relevant written submissions (deleting or redacting any commercial-in-confidence or personal information) received.

We would also suggest that a comment period of 28 days is unduly short: we would instead recommend a minimum comment period of 60 days, which could be divided if the code developer elected to release two drafts.

6. Civil penalties under Section 80Z

The extent to which an entity is liable under section 80Z for multiple penalties (if the same facts give rise to more than one contravention) should be further clarified either in the Proposed Law or Explanatory Memorandum.

Subsection 80Z(1) states that the court may make a single order against an entity for multiple contraventions of a civil penalty provision if proceedings for the contraventions are founded on the same set of facts. Subsection 80Z(2) does not preclude the application of multiple penalties.

Where multiple penalties apply, we submit that it should be clear that a 'totality' principle should be used to provide an appropriate boundary in enforcement proceedings. For example (and in a different but analogous context) enforcement proceedings under the *Competition and Consumer Act 2010* (Cth) have considered whether, in the face of multiple penalties, the penalties imposed for multiple penalties are, in aggregate, just and appropriate (for example, see *ACCC v McMahon Services Pty Ltd* [2004] FCA 1171 at [91] per Lander J).

A clarifying amendment could be made by inserting a new subsection 80Z(3) codifying a 'totality' principle. Alternatively the prospective application of the totality principle should be noted in the Explanatory Memorandum.

7. Requirements of foreign laws

Consistent with the global digital economy in which online services operate, an entity may be regulated under Australian privacy law and also regulated under foreign laws. These organisations will of course need to comply with laws in the countries from which they operate and in which they collect and hold personal information about individuals.

For example, a foreign country may mandate disclosure of personal information in response to a subpoena issued by a court exercising jurisdiction over the operations of the service provider. It would be inappropriate to place the service provider in jeopardy under Australian law for responding to valid court process in a foreign jurisdiction.

Another example would be a law requiring service providers to disclose the details of a person alleged to have engaged in illegal activities, such as the duty of a service provider to report instances of child pornography as set out in section 2258A of 18USC (http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1476#6).

There are a number of provisions in the APPs that, we believe, do not adequately allow for the requirements of foreign laws. These are APP3.4, APP5.2(c), APP6.2(b), APP8.2(c), APP11.2(d) and APP12.3(g). To illustrate by an example, APP8 (cross-border disclosure of personal information) does not in terms address disclosure of personal information made by an APP entity or an overseas recipient pursuant to requirements of an applicable law of a foreign country.

The lack of an acknowledgement within the Proposed Law of the need to comply with foreign laws jeopardises the ability of digital economy companies to be responsive to legal requirements where they operate in other countries. In addition, if other countries were to adopt similar laws (ie constraining compliance with foreign laws), then Australian legal requirements may be similarly frustrated.

We think the following amendments would provide much needed certainty for organisations:

- the Explanatory Memorandum should provide clarification about the scope of the term "applicable law of a foreign country", such that a court/tribunal order of a foreign country is clearly a requirement of an applicable law of a foreign country; and

- sections 6A(4), 6B(4) and 13D should be amended to more clearly acknowledge that an act done or a practice engaged in within Australia to comply with the requirements of a

foreign law directly applying to that organisation cannot be deemed to be a violation of Australian law.

In relation to the first point, a new distinction is drawn by definitions added by the Proposed Law between an "Australian law" and a "court/tribunal order", as used in various places in the Proposed Law but relevantly in proposed APP8.2(c). Because APP8 does not in terms address disclosure of personal information pursuant to requirements of an applicable law of a foreign country, an APP entity or an overseas recipient compelled by foreign law to make a disclosure must rely upon existing sections 6A(4), 6B(4) or 13D, as each are relevantly amended by the Proposed Law. However, these provisions use the omnibus expression "applicable law of a foreign country", in relation to which expression there is now some ambiguity because of the new distinction between an "Australian law" and a "court/tribunal order" that has been introduced by the Proposed Law. Specifically, is a court order of a foreign country also a requirement of an applicable law of a foreign country?

We think it would be useful, and entirely consistent with announced Government policy, if the Explanatory Memorandum stated that "applicable law of a foreign country" is (still) intended to cover the requirements of court orders, directions of regulatory agencies and other legally enforceable instruments made pursuant to an applicable law of a foreign country, as well as any direct application of that foreign law.

As to our second point, we note that sections 6A(4), 6B(4) or 13D only cover an act done or a practice engaged in outside of Australia. Where an organisation acts within Australia pursuant to requirements of foreign law that directly apply to that organisation, that organisation should not be placed under jeopardy of Australian law when that organisation acts within Australia to meet the requirements of a foreign law directly applying to that organisation. We request that consideration be given to amending sections 6A(4), 6B(4) and 13D to cover an act done or a practice engaged in within Australia to comply with the requirements of a foreign law directly applying to that organisation.

Finally, given the importance of sections 6A(4), 6B(4) and 13D we request that the Government give consideration to confirming its intention that that these sections will remain in materially the same form as proposed in the Proposed Law through the process of implementation of the current reform package. This assurance would provide greater certainty to industry and build confidence in the new privacy regime.

Conclusion

In conclusion, the Submitters remind the Committee of our strong commitment to privacy. If people do not trust our services and if they do not have positive experiences on the platforms we provide then we do not be successful in fulfilling our respective missions and users will switch to a different service.

When finalising its recommendations about the proposed reforms, we encourage the Committee to take account of the considerable benefit that online services bring to the Australian economy. A recent study estimated that the direct contribution of the internet to the Australian economy was worth approximately **$50 billion** or 3.6 per cent of GDP in 2010[6]. That is expected to increase by at least $20 billion over the next five years to **$70 billion**[7], although the study authors suggest that this estimate may well turn out to be on the low side in light of the fact that it is currently impossible to predict the myriad of applications that will be made possible by broadband connections.

In addition, the Australian Government has identified the digital economy as being "essential to Australia's productivity, global competitiveness and improved social well being", and, as outlined above, has set itself the goal of becoming one of the world's leading digital economies by 2020[8].

To continue to enable online services to deliver benefit to Australian households and businesses, and to ensure that the Australian Government achieves this goal, we invite the Committee to make recommendations that ensure that Australian privacy laws are enhanced and future-proof in a way that is appropriately balanced and permissive of innovative and global digital economy services.

Thank you once again for the opportunity to provide feedback on these amendments. Should you wish to discuss any of our comments don't hesitate to contact us.

Mia Garlick
Head of Policy and Communications
Facebook Australia & New Zealand

Ishtar Vij
Policy Counsel
Google Australia & New Zealand

Samantha Yorke
Director of Regulatory Affairs
IAB Australia

Nick O'Donnell
Regional Manager, Public Policy APAC
Yahoo!7

---

[6] The Connected Continent: How the internet is transforming the Australian economy, Deloitte Access Economics,August 2011 https://www.deloitteaccesseconomics.com.au/uploads/File/DAE_Google%20Report_FINAL_V3.pdf , p2
[7] Ibid p46
[8] National Digital Economy Strategy