Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Committee Secretary
Senate Standing Committee on Environment and Communications
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

21 December 2010

Re: Online Privacy Inquiry - Supplementary Submission from the Australian Privacy Foundation and response from the Attorney-General's Department

I refer to the letter to the Committee from the Attorney-General's Department, dated 16 December, which quotes from an article I wrote in 2008 (the date is not mentioned in AGD's letter) in my capacity as a Visiting Fellow at the Cyberspace Law & Policy Centre, Faculty of Law, University of New South Wales (the paper is online at http://www.law.bepress.com/unswwps/flrps08/art59/).

While the quotation is accurate, it is selective, dated and lacks context. The Department appears to present it as a rebuttal of the criticism of the APEC privacy initiative contained in the supplementary submission from the Australian Privacy Foundation (APF) (published by you as part of Submission No 14).

The Committee should be advised that I do not regard either the quotation itself, or my views then and now, as in any way inconsistent with the APF criticisms. Indeed, as a Board member of APF I have contributed to the formulation of the Foundation's position in relation all current inquiries, including both yours and that of the Senate Finance and Public Administration Committee into the Exposure Draft Australian Privacy Principles, which is also relevant to the point at issue.

At the end of the quoted passage, I said:

> *"Of greater practical significance is the way in which the obligations are firstly embodied in domestic law and secondly enforced."*

In respect of the first of these – domestic law – I continue to harbour significant fears.

In the same paper, I wrote:

> *"There are too many 'lines in the sand' drawn by the domestic laws of key trading countries to allow either the APEC initiative or any other developments to undermine existing privacy protection standards. For this to occur, laws in Europe, Australia, Hong Kong, and possibly soon in other APEC countries mentioned above as bringing forward legislation, would need to be amended to weaken their limits on cross border transfers. This is not in prospect in any country[53], and seems unlikely"*

The footnote (53) was to the then still in progress ALRC Privacy Inquiry.

Regrettably, both the ALRCs final report and the government's subsequent response to it have re-awakened fears of a weakening of Australian law in relation to cross border transfers.

Detailed criticism of the government's proposed Australian Privacy Principle 8 (cross-border disclosure ...) by myself and Professor Greenleaf is contained in the Cyberspace Law & Policy Centre submission (and endorsed in the APF submission) to the current Senate Finance and Public Administration Committee inquiry into the Exposure Draft APPs (http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/submissions.htm).

For the purposes of this letter, it is sufficient to emphasise that the fears expressed in the APF's Supplementary Submission and by Dr Clarke in verbal evidence are very real and justified.

In my 2008 paper, I drew attention to the stated position of the Australian government in 2003, in relation to the APEC initiative, that:

> *"... The Australian view is that there is no need for any externally imposed test of adequacy for member economies[54]"*

The subsequent history of the APEC privacy initiative has been one of a continued tension between the desire of some member economies – principally the US but also to some extent Australia – to maximise the role of private sector self-regulation as a way of implementing the APEC Privacy Framework, and the growing recognition by other economies of the need for binding and enforceable privacy laws. As a civil society observer at APEC Privacy Subgroup meetings[1], I have closely observed the playing out of this tension.

In my latest published commentary on the APEC work[2], I emphasise the continued uncertainty over the governance arrangements for the Cross Border Privacy Rules (CBPR) system that is being developed as one way of implementing the APEC principles. There remains a risk that the CPBR system will accommodate and endorse weak privacy laws in some member economies and effectively require other members to allow transfers of personal information with a consequent loss of privacy protection.

If the proposed APP8 is enacted unchanged, this would give substance to the APF supplementary submission that *"If any aspects of this empty model were to be implemented in Australia, there would be a massive reduction in protections"*. While the overall APEC model has some positive features, I share the concern that a combination of the proposed amendment to the Australian law with the APEC Cross

[1] I represent Privacy International at these meetings – my last report is at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566294

[2] *Critical elements unresolved in APEC cross border privacy rules*, Privacy Law and Business International Newsletter 107, October 2010 (access by subscription only – article attached)

Border Privacy Rules system, if it is eventually adopted, could indeed lead to a significant weakening of privacy protection for all Australians.

I hope this letter serves to set the record straight and corrects the impression that may have been given to the Committee that my position differs in any significant respect from that of the Australian Privacy Foundation.

Yours faithfully

Nigel Waters
Visiting Fellow
Cyberspace Law & Policy Centre, Faculty of Law, UNSW
http://www.cyberlawcentre.org/

Attachment – article from Privacy Laws and Business International Newsletter, No 107, October 21010

Critical elements unresolved in APEC cross border privacy rules

Nigel Waters reports from September's APEC Privacy Framework Meeting in Japan.

There has been limited progress on the Pathfinder Projects, designed to set up a system of APEC Cross Border Privacy Rules (CBPR), which has been the main focus of the Data Privacy Subgroup's work programme since 2007 (*PL&B International*, August 2010, p. 15). The self-certification questionnaire for organisations seeking to join the CBPR system (Project 1) and the recognition criteria for Accountability Agents (AAs) (Project 2), were finalised and endorsed – the AA recognition criteria having been revised to now apply to both private and public sector accountability agents, and to recognise that the required dispute resolution mechanism may be provided by a specialised third party under a contract or agreement. The compliance review guidelines for Accountability Agents to use in assessing applications from organisations (Project 3) were subject to detailed editing, but several member economies want to further consider the final draft and it will not be possible to formally endorse these guidelines before the next round of meetings in Washington DC, USA, in early 2011.

Other administrative components have already been endorsed (Projects 5, 6 & 7) and the cross-border enforcement cooperation arrangement (Project 6) has now commenced. The major outstanding component of the CBPR system is agreement on overall governance and administrative infrastructure (Project 8). Difficult issues arising from other projects – particularly Project 2 – have been carried over into Project 8, which will now review, out of session, a paper to be drafted by the US Department of Commerce. Outstanding issues to be resolved include mechanisms for accrediting privacy enforcement authorities (PEAs) and accountability agents (AAs); the identity, status and role of the proposed Joint Oversight Panel governance body, and funding – i.e. revenue generation and sharing (likely to be a significant hurdle to be overcome). Associated with this is the requirement for a public website listing organisations certified as compliant under the CBPR system (Project 4) – work is continuing on a specification for this website which is expected to be hosted by the APEC Secretariat but will need to fit into the overall governance and funding arrangements, once agreed.

Enforcement cooperation

The Cross Border Privacy Enforcement Cooperation Arrangement (CPEA) was launched on 16 July 2010. It is not limited to the CBPR system and is available for any cooperation on any privacy complaints or investigations by participants. The first five signatories – participating privacy enforcement authorities (PE Authorities) – are the Australian, New Zealand, Canadian and Hong Kong Privacy Commissioners and the US Federal Trade Commission. The Australian, NZ and US regulators, supported by the APEC Secretariat, are initially jointly performing the role of CPEA Administrator, including assessing applications to join the CPEA from other PE Authorities.

Because common criteria have been used and mutual recognition arrangements established, eligibility to join the CPEA automatically qualifies a PE Authority to join the Asia Pacific Privacy Authorities forum (APPA). The CPEA is also designed to be consistent with the emerging OECD Global Privacy Enforcement Network (GPEN) (*PL&B International*, June 2010, p. 18).

The public launch of the CPEA, and the fact sheet about it now readily available on the APEC website, mark a new level of transparency for the APEC privacy work. However, while the CPEA is a potentially valuable initiative, it will only be effective if it is actually used to resolve privacy complaints with a cross-border element, and it remains to be seen if the participating PE Authorities will put the necessary resources and commitment into making it work.

Practical value?

Whether the APEC CBPR system proves to be of any practical value will depend on the finalisation of the governance arrangements, which will be the focus of the Data Privacy Subgroup's work over the next year. The intention remains to have the CBPR system completed and operational by the end of 2011.

As well as the CBPR work, and establishment of the CPEA, the Data Privacy Subgroup also seeks to encourage domestic implementation of the APEC Privacy Framework in member economies. The Subgroup meeting and the technical assistance seminar in Japan heard reports on developments in several countries, including passage of a data protection law in Malaysia (*PL&B International*, April 2010, p. 1) and Mexico (*PL&B International*, June 2010, p. 1), progress towards legislation in Thailand, the Philippines, Chile and Peru, and proposed amendments to existing privacy laws in Australia, Chinese Taipei, Hong Kong (China), South Korea and Canada. Other delegates reported associated developments with Trustmark schemes and/or relevant sectoral legislation, and, in the case of the USA, the FTC's work on Online privacy.

The Subgroup also heard reports on related international developments in the OECD, APPA and on the Accountability project's 2010 Paris phase and ambitions for 2011, which overlaps with the work of the EU's Article 29 Working Party summarised in its Opinion 3/2010 on the principle of Accountability.

AUTHOR

Nigel Waters of Pacific Privacy Consulting attended the APEC Privacy Framework meeting in Japan as an invited guest, with a watching brief on behalf of Privacy International (PI) and support from PI's Privacy in Asia project.
Email: nigelwaters@pacificprivacy.com.au