APEC Privacy Enforcement Workshop, Auckland, NZ, 17-18 July, 2013

Session: APEC Cross Border Privacy Rules System: How does CBPR enforcement work for consumers, business and privacy enforcement authorities?

Nigel Waters[1]

I will address the part of the question that goes to how CBPR enforcement will work for *consumers*. The short answer is that it is too early to tell – the CBPR system is still 'under construction' and the first certification of businesses under the system won't occur until later this year, probably in the US, and will only take practical effect for cross border data transfers between two participating jurisdictions – only the US and Mexico currently qualify, with Japan having applied. Enforcement will take longer – there will need to be either complaints or allegations about breaches of the program requirements, which are the standards that certified businesses will be held to, consistent with the Principles in the APEC Privacy Framework.

What are the prospects? The APEC CBPR system is intended to work for consumers in two ways. The primary objective is to ensure that a minimum standard of privacy compliance applies to transfers of personal information between participating APEC economies. In some cases, domestic laws will require a higher standard, both of handling in the country where the information is collected and in respect of any cross border disclosures.[2]

CBPR certified businesses will be able to hold themselves out to consumers as meeting the standard (programme requirements consistent with the Principles in the APEC Privacy Framework, adopted in 2005). They will be held to account initially by an Accountability Agent which assesses their application and certifies them. The US privacy seal programme TRUSTe has been accepted as the first recognised Accountability Agent, which will be offering a yet to be fully defined new CBPR privacy seal.

The second way in which the CBPR system is intended to work for consumers is in the event of a breach of the privacy standards – such as a loss or misuse of personal information held or processed by a CBPR certified business involving a second jurisdiction. Certified businesses voluntarily accept the jurisdiction of the relevant Accountability Agent, which must offer External Dispute Resolution, and will also be subject to investigation and enforcement action by the Privacy Enforcement Authority (PEA) – economies cannot participate without a law under which the CBPR programme requirements can ultimately be enforced, and a PEA with the necessary powers to do so. PEAs must also be members of the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

In a cross border data transfer context, it will often be difficult if not impossible to know who is responsible for a breach of privacy and where the breach occurred (geographic location is an elusive

---

[1] Principal, Pacific Privacy Consulting www.pacificprivacy.com.au , Board member of the Australian Privacy Foundation www.privacy.org.au , and former Australian Deputy Privacy Commissioner. He has attended most meetings of the APEC Data Privacy Subgroup since 2006, representing international Civil Society.

[2] For example, privacy laws in Australia, New Zealand and Hong Kong contain express conditions for cross border data transfers. In other APEC privacy laws (e.g. Canada) there is an implicit requirement for appropriate cross border conditions under a general security principle.

concept in many globalised data processing businesses). The intention is that an aggrieved individual will be able to complain to the PEA in their own country which will liaise with the PEA (or directly with the AA) in the other jurisdiction involved in the processing. The initial task will be to identify which data controller in which country needs to take responsibility. The AA in the relevant jurisdiction will be expected to seek to resolve the complaint with the certified business concerned. In the event that resolution is not achieved, the complainant should be able to escalate it and have it investigated by one or both PEAs, leading ultimately to a formal finding and to any financial or other remedies sanctions or penalties which may flow.

The difficulties of cross border privacy enforcement cooperation are not confined to the APEC CBPR system – PEAs around the world have been struggling to deal with cross border complaints for many years – and have only recently started to adopt consistent joint approaches to allegations about the privacy practices of global businesses such as Google, Microsoft, Sony and Facebook.

A Global Privacy Enforcement Network (GPEN), with its origins in the OECD, predates the APEC CPEA and there is increasing cooperation more generally through the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and regional equivalents such as the Australia Pacific Privacy Authorities (APPA).

This cooperation, particularly through GPEN and APEC CPEA, includes detailed procedures and protocols for complaint handling, but these have yet to be tested in practice. Consumers will only be satisfied if they have easy access to processes which deliver effective remedies for privacy breaches and which do not take an inordinately long time. Experience within most jurisdictions does not set an encouraging precedent, with most CPEAs (Privacy Commissioners or equivalent bodies) having significant complaint backlogs and taking months if not years to finalise more difficult complaints.

Part of the promise held out for the CBPR system is that many complaints should be resolved earlier – if not by the businesses involved, then by the Accountability Agent's EDR processes, without needing to engage the often slow and bureaucratic PEAs.

Consumers in most countries are however very sceptical about the performance of 'self-regulatory' regimes in general, and this scepticism extends to self-regulatory elements of privacy protection. An analysis of privacy seal programmes by Galexia Consulting in 2008[3] found many failings, and a more detailed analysis of the Safe Harbor scheme accepted by the EU as offering adequate protection was also highly critical.[4]

In the CBPR context, international civil society is particularly concerned at the precedent set by recognition, in June 2013, of the US seal programme TRUSTe as the first Accountability Agent in the CBPR system. Even if the certification requirements for CBPR privacy seal (which is still a work in progress) meet the CBPR programme requirements, it is difficult to see how TRUSTe will be able to apply a level of scrutiny to applications that will ensure compliance. Also, the US implementation of the CBPR system relies on 'backstop' enforcement by the Federal Trade Commission. Under Section 5 of the FTC Act, 15 U.S.C. § 45. The FTC has broad authority to take action against unfair and deceptive acts and practices. Unlike privacy enforcement regimes in most countries, enforcement of CBPR in the US would be indirect – action would not be for breach of a programme requirement but for failing to honor promises made by committing to the TRUSTe privacy programme requirements.

---

[3] Connolly C, *Trustmark Schemes Struggle to Protect Privacy*, October 2008, <http://www.galexia.com/public/research/articles/research_articles-pa07.html>.
[4] Connolly C, *The US Safe Harbor - Fact or Fiction?*, December 2008, <http://www.galexia.com/public/research/articles/research_articles-pa08.html>.

While the FTC has successfully brought some privacy actions under section 5 against US businesses, it remains to be seen whether this mechanism will offer a satisfactory enforcement path for all types of breaches.

At the APEC Data Privacy Subgroup meeting in Sumatra in June 2013, this author made a statement on behalf of international civil society about the recognition of TRUSTe, setting it in the wider context of US led attempts to redefine privacy protection in several international forums. The statement is appended to this paper.

Civil society NGOs, and ultimately all consumers in APEC member economies, will be disappointed if other economies join the CBPR system with combinations of Privacy Enforcement Authority and Accountability Agent(s) which have similar weaknesses to those that appear in the US FTC-TRUSTe combination. It seems that privacy seal or trustmark programmes in economies such as Mexico, Japan, Chinese Taipei, Singapore, Malaysia and Vietnam[5] are considering applying for AA status once their governments have become participants (Mexico already has and Japan has applied). Some of these countries already have specific privacy or data protection laws which include cross border data transfer controls, and businesses will have to comply with those laws independently of any participation in the APEC CBPR system. One of the fears of civil society is that privacy laws could be amended to recognise CBPR participation alone as an 'adequate' basis for cross border data transfers, when this clearly represents a lower standard of protection.

Criticism of the CPBR system should not be taken as implying satisfaction with the alternative legislated enforcement regimes in those countries that have such laws. In most laws, there are structural weaknesses in the powers of PEAs, the range of remedies and sanctions and the procedural provisions for complaints. Equally important are the failure of governments to adequately resource PEAs, and the failure of many PEAs to effectively deploy their resources and to exercise the powers they do have, in terms of both pro-active compliance monitoring and complaints resolution.

But at least in legislated frameworks there are generally opportunities for legal challenges. One of the fears that civil society has about the APEC CBPR system is that it may result in either implicit or explicit 'outsourcing' of most compliance monitoring and complaints resolution to self-regulatory intermediaries, with pressure on aggrieved individuals to accept mediated outcomes as 'good enough' even where they are not satisfied, or where interpretations of privacy principles really need to be tested and binding precedents set.

It is possible that the concerns expressed by civil society about the APEC CBPR system, and in particular about its current implementation, will be proved groundless. It could be that the system results in businesses taking a much more proactive approach to privacy compliance in order to obtain certification than they are required to even in countries where they are subject to privacy laws. Accountability Agents may carry out more routine monitoring and dispute resolution than a poorly resourced PEA could ever do, leaving the PEA to focus on major and systemic problems. Any or all of these outcomes could contribute to an overall higher level of privacy protection for consumers. We live in hope!

[5] The World Trustmark Alliance represents these programmes in and is actively involved in the CBPR related work of the APEC Data Privacy Subgroup

The APEC Cross Border Privacy Rules system: A Civil Society perspective, June 2013

The following statement was made to the APEC Data Privacy Subgroup[6] meeting on 24 June 2013, in Medan, Sumatra, by Nigel Waters[7], attending the meeting as an invited guest. At previous meetings Mr Waters has represented Privacy International, but due to difficulties in obtaining guest status for PI (or other privacy or consumer NGOs) he has attended the last two meetings in an individual capacity. In the absence of a formal multi-stakeholder mechanism, he seeks to bring the perspective of international civil society[8] to bear in the APEC privacy work.

"The most significant development since the last DPS meeting has been the approval of TRUSTe as an Accountability Agent (AA) under the CBPR system. It is unfortunate that it was left to civil society volunteers to question the JOP assessment of the TRUSTe application for recognition as an AA. We are pleased that a number of economies took up some elements of our critique. This appears to have led to some specific modifications to the application (and consequently to the JOP's report) but also to many assurances about future changes and TRUSTe practices, which the JOP has taken on trust. We consider that the changes and assurances (even if subsequently delivered) fail to address the most serious criticisms, and we cannot understand how the JOP, and member economies, can be satisfied that the application met the recognition criteria.

International civil society believes that approval of TRUSTe as an Accountability Agent has seriously undermined the credibility of the CBPR system. It is a very unfortunate precedent, setting a low bar for other applicants for AA recognition both in the US and in other economies. The TRUSTe model, in association with an enforcement arrangement based on Trade practices law rather than mandatory privacy principles, means that compliance with the CBPR system in the US will essentially rely on self-assessment, with minimal pro-active oversight or independent checks. Any prospective market for effective private sector Accountability Agents has been undercut by a largely token certification program from an organisation with a questionable track record.

This development needs to be seen in the context of intensive lobbying by business interests, aided by some governments, to weaken privacy and data protection laws around the world, not least through reviews of the key international privacy instruments – the OECD Guidelines, the Council of Europe Convention 108 and the EU Directive and proposed Regulation. At stake is the ability of privacy laws to do any more than require 'good housekeeping' of personal data. The critical role of current laws in challenging the legitimacy of some business models and practices is under threat. Business interests seek to ensure that privacy laws do not limit their ability to use personal data for secondary commercial purposes without express consent, and to move data around the world unconstrained by the absence of strong privacy protection in some jurisdictions. The campaign for 'interoperability' needs to be recognised for what it is – an attempt to gain mutual recognition of different privacy protection regimes with a very low 'floor' or entry threshold.

These efforts to shift the balance in privacy protection away from individual control towards business interests, so far successful in the APEC CBPR system, stand in stark contrast to the steady growth of strong domestic privacy laws around the world, including in APEC – at the last count, 93 jurisdictions with laws applying to the private sector[9]. Countries continue to adopt privacy laws because of the clear evidence that they are essential for long term trust in electronic commerce, which is a shared goal. The CBPR system could, if redirected, contribute to this trend rather than undermine it. Civil society will continue to closely monitor the direction of the system, and of APEC privacy implementation more generally, and will continue to urge APEC members to raise rather than weaken standards of privacy protection."

---

[6] See http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx

[7] http://www.pacificprivacy.com.au/Biography%20and%20CV.htm

[8] Mr Waters is on the Advisory Board of Privacy International https://www.privacyinternational.org/ and is a member of the steering committee of the OECD Civil Society Information Society Advisory Council http://csisac.org/ He can be contacted at board5@privacy.org.au

[9] See Greenleaf 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877