# APEC's CBPRs in operation for two years: Low take-up, and credibility issues

Graham Greenleaf , Professor of Law & Information Systems, UNSW Australia, and
Nigel Waters, Director, Pacific Privacy Consulting*

(2014) 129 *Privacy Laws & Business International Report*, 12-15

APEC's CBPRs, like any other form of regulation, cannot simply be assumed to be credible and effective. In addition to its professed standards (considered in the previous article, G Greenleaf (2014) 128 PLBIR, 27-30), its operation in practice must be examined to determine whether it credibly upholds and enforces those standards. APEC's Cross-Border Privacy Rules system (CBPRs) is not yet in full operation, but the initial operation of any institution is often a major determinant of its future path. The first two years of APEC CBPRs operation is examined in this article and found wanting.

## The first two years of operation: a slow start

The APEC CBPRs rules were completed in 2011.[1] By mid-2014, three of the 21 APEC economies, the United States, Mexico and Japan, had reached different stages in becoming participants in the CBPR system, and Canada has indicated it intends to start the process. The process to become a participant requires completion of four matters to the satisfaction of APEC's Joint Oversight Panel (JOP)[2]: (i) confirmation from the economy's 'Designated APEC Government Delegate' that the economy intends to participate; (ii) the appointment of a Privacy Enforcement Authority (PEA) by the economy, which then notifies its intent to participate in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) system; (iii) the JOP issues a 'Findings Report' approving the economy's participation on the basis that it has 'laws and regulations … the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework', and (iv) the forwarding of an Accountability Agent (AA) application to JOP by the economy, and its approval by the JOP. In relation to the 'Findings Report' there is no opportunity for other economies to object, but all economies are given an opportunity to object to an AA appointment. Final approval is decided by JOP but announced by its parent body, the Electronic Commerce Steering Group (ECSG).

Announcements of each step in an economy's participation are on the CBPRs website.[3] Once these steps are completed, the AA can start to certify companies as CBPR-compliant, and to enforce the obligations of certification against such companies. The extent of participation of each of the three is now analysed. The US, the first and as yet only full participant, is discussed last.

* Thanks to Chris Connolly for valuable comments. Responsibility for content remains with the authors. The authors have also contributed, with Chris Connolly, to the CS submission and the APF submission referred to in this article.

[1] The CBPR system and documents were endorsed by Ministers at their 2011 Meeting in Honolulu, and APEC Leaders committed to implementing the CBPR System in their 2011 Declaration. The intake documentation was first used by the USA in July 2012

[2] JOP is currently comprised of representatives of the US (chair) Japan, Australia, and Mexico, from which a JOP of three is drawn in relation to a particular application.

[3] Primarily <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx> and also <http://www.cbprs.org/GeneralPages/LatestNews.aspx>

## Mexico: Still in progress

In September 2012 Mexico's relevant Ministry (called in brief 'Economia') confirmed its intention to participate and that Mexico's data protection authority (IFIA) would be its PEA, and was a participant in CPEA.[4] Mexico has not yet nominated an AA for JOP approval, but these first two steps are sufficient for APEC to regard it as 'participating' even without an AA. A brief 'Findings Report' by the JOP concerning Mexico in January 2013[5] noted that

> Article 44 of Mexico's *Federal Law on Protection of Personal Data held by Private Parties* provides that persons or entities may agree on binding self-regulatory schemes in addition to the requirements of the Law itself. Chapter VI provides that these binding self-regulatory schemes may include third-party certification of those responsible for the protection of personal data in accordance with certification parameters established by Economía, with the support of IFAI. Article 43 grants Economía and IFAI the authority to establish and enforce these parameters, including rules governing the Certification System and the certification-related activities of third-party certifiers. Further, IFAI is granted the authority to authorize the accrediting entities that will be in charge of accrediting such certifiers.

Apart from this statement, and noting that Mexico has filed an outline of its laws and the required 'Enforcement Map', the JOP does not detail any substantive or independent assessment of those laws or the Enforcement Map. However, it does make a formal finding that the conditions 'establishing the requirements for recognition as a Participant' in APEC CBPRs 'have been met by Mexico'. The JOP's Charter instructs it only to consult with the economy concerned, not with anyone who might provide an independent viewpoint on the substance of an economy's compliance, and that is all that JOP says it did. While it does seem that Mexico's law is well-suited to mesh with the APEC CBPRs, this JOP procedure seems close to self-assessment by Mexico, in the absence of JOP consulting with anyone other than official representatives of the economy concerning. We are not suggesting that Mexico does not comply in substance, only that the JOP process is inadequate to establish this.

## Japan: 16 'PEAs in a pod' and perhaps up to 39 AAs

In June 2013, officials from two Japanese Ministries advised APEC ECSG of Japan's intent to join the CBPRs,[6] and that it would have no less than 16 PEAs (enforcement authorities).[7] The 'sixteen PEAs in a pod' do not include Japan's new 'mini-DPA' (see (2014) 128 PLBIR, 10-12), which is not yet operational. A Findings Report by the JOP[8] confirms that Japan has appointed these 16 PEAs, and 'intends to make use of at least one APEC-recognized' AA. It has not yet nominated an AA for JOP approval, but from the Findings Report it is possible to infer what is likely to happen. The Findings Report is of the same nature as for Mexico: it confirms that Japan has filed the necessary documents, and it says the JOP consulted with relevant Japanese government bodies (and

---

4 'Mexico's Letter of Intent to Participate in CBPR' (APEC ECSG, 2013) <http://www.apec.org/%7E/media/Files/Groups/ECSG/Mexico-Letter-of-Intent_CBPR.zip>.

5 'JOP Findings Report regarding Mexico's intent to participate in the CBPR system' (JOP, 16 January 2013) <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>

6 Ministry of Economy, Trade and Industry (Japan) 'The Government of Japan Applied to Join the APEC Cross-Border Privacy Rules System' (METI, 7 June 2013) <http://www.meti.go.jp/english/press/2013/0607_03.html>.

7 A Japanese body confirmed a slightly different list of 16. by a letter on APEC letterhead dated 5 February 2014 addressed to the Chair of the JOP from Japan's 'Framework Administrators of the APEC CPEA' (no Ministry or address specified). The 16 PEAs are the Ministry of Foreign Affairs; Ministry of Economy, Trade and Industry; Ministry of Internal Affairs and Communications; Ministry of Finance; Ministry of Justice; Ministry of Agriculture, Forestry and Fisheries; Ministry of Land, Infrastructure, Transport and Tourism; Ministry of Defencse; Ministry of Health, Labour and Welfare; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Environment; Cabinet Office; Consumer Affairs Agency; Financial Services Agency; National Police Agency; Reconstruction Agency of Japan.

8 'JOP Findings Report regarding Japan's intent to participate in the CBPR system' (JOP, 25 April 2014) <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>

the CPEA administrators). JOP did not consult with anyone else, or make any independent assessment of the substance of Japan's law and its implementation over ten years.

Concerning AAs, the Findings Report says:

> Under Article 46 of Japan's *Act on the Protection of Personal Information*, a competent Minister may require an authorized personal information protection organization ("Accountability Agent") make a report regarding its privacy-certification related practices. Additionally, under Article 47, a competent Minister may order the Accountability Agent to "improve its methods of conducting its authorized businesses, amend its personal information protection guidelines, or to take any other necessary measures to the extent necessary for implementation of the provisions of this section." Should an Accountability Agent fails to obey this order, a competent Minister may rescind the authorization of that Accountability Agent to operate in Japan pursuant to Article 48(1). In this case, the Accountability Agent is prohibited from any certification-related activities as part of the CBPR system. Through this authority, Japan may nominate and submit to the ECSG, the DPS and the JOP, the relevant application and associated documentation of those accredited certifiers seeking APEC recognition as an Accountability Agent in the APEC CBPR System.

This implies that only an 'authorized personal information protection organization' (APIPO) under the Act (they are not called 'Accountability Agents' therein) can be nominated to be an AA. APIPOs are industry-based self-regulatory organisations, and there are 39 of them. The Report omits to state that, ten years after Japan's legislation was enacted, only one Ministerial order (in 2007) is known to have been given to any of the 39 APIPOs, and in no case has the operation of an APIPO been rescinded. Although APIPOs can receive complaints from members of the public against their members, they have no independent powers. They are not arbitrators in disputes or even specifically empowered to be mediators. They are not known to have had any effect in enforcing Japan's privacy laws.[9] Japan might therefore be intending to nominate up to 39 Accountability Agents, but probably less depending on which industries want to be part of APEC CBPRs, or are induced to participate. This helps explain the 16 PEAs, because only the relevant Ministry for a particular APIPO could (in theory) force it to do anything. Since a main function of an AA is to receive and resolve complaints from foreign individuals whose personal data has been transferred to an AA-certified Japanese company, it is a matter of speculation how any of the 39 APIPOs, who only operate in Japanese, will ever be found, or how any foreigners will ever work out which AA and which PEA are relevant to their complaint. It is also possible that JIPDEC, Japan's 'trustmark' provider, which operates through 18 'Conformity Assessment Bodies' could become an AA. However, JIPDEC's track-record of enforcement against its members, or transparency, is little better than that of the APIPOs and no-more likely to be understandable by data subjects outside Japan.[10] APEC's JOP has simply ignored these unrealistic elements of Japan's proposal. This indicates that APEC JOP approvals may have insufficient grounding in substance and reality.

The 'Enforcement Map' in the Findings Report is intended

> to identify all relevant provisions in the Act on the Protection of Personal Information (herein 'Act'), the Cabinet Order for the Enforcement of the Act on the Protection of Personal Information (herein 'Cabinet Order'), and the Basic Policy on the Protection of Personal Information (herein 'Basic Policy'), relevant to the enforceability of each of the 50 CBPR program requirements.

The problem is that this Map, by itself, is a purely formal recital of what Japan's law says, according to the Japanese government. JOP makes no reference to alternative critical interpretations, and no attempt to assess whether there is any reality in the enforcement aspects. Critics have argued that, by and large,

---

[9] G Greenleaf and F Shimpo 'The puzzle of Japanese data privacy enforcement', (2014) 4(2) *International Data Privacy Law*, 139-154, < <http://idpl.oxfordjournals.org/content/4/2/139.full.pdf+html>, section 7.1; see also earlier criticisms cited therein.

[10] G Greenleaf and F Shimpo 'The puzzle of Japanese data privacy enforcement', section 7.2.

there is little or no enforcement[11]. While there is plenty of room for differing opinions about Japan's laws, the JOP Report is not an independent assessment, it is simply a formal assessment by officials of governments committed to APEC CBPRs, that, in theory, Japan's laws have the elements required by APEC. These deficiencies are more clear from the Japanese example than that of Mexico.

This APEC process should not be equated with the more independent and substantive processes carried out by the EU ('adequacy assessments'), or even the more recent (and still developing) assessment processes carried out by the Council of Europe in its 'globalisation' of Convention 108. Those processes are also open to criticism, but not to the same extent as the APEC CBPRs processes.

## The sole full participant: The dubious precedent of the US

The US is the only applicant to have yet finished the process to be a participant, having completed to the satisfaction of the JOP[12] the required steps.

The US company TRUSTe has been approved as an Accountability Agent for the US by the JOP,[13] but only after civil society organisations intervened following the initial JOP recommendation of approval, and caused a number of economies to call for reconsideration, eventually resulting in an amended Final Report by JOP which recommended approval on the basis that TRUSTe would make various changes. Waters, a guest attendee at the following APEC Data Privacy Subgroup meeting, stated that civil society organisations were very critical of what they saw as the JOP's 'rubber stamp' approval of TRUSTe's application:[14]

> 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.

A civil society submission to the JOP[15] after its initial recommendation of approval of TRUSTe[16] argued that TRUSTe's application had many deficiencies, including, that TRUSTe's program standards/requirements, failed to meet at least 21 of APEC's program requirements,[17] that it

---

[11] G Greenleaf and F Shimpo 'The puzzle of Japanese data privacy enforcement'.

[12] 'JOP Findings Report regarding USA's intent to participate in the CBPR system (JOP, 25 July 2012) <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>

[13] CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013, as amended 18 June 2013); See also other documents concerning appointment of TRUSTe as Accountability Agent (APEC ECSG, 2013) <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx> accessed 14 January 2014; Other documents included are; 'TRUSTe - Annex B: Accountability Agent Recognition Criteria Checklist'; and 'TRUSTe - Annex C: APEC Cross-border Privacy Rules System Program Requirements Map'.

[14] Nigel Waters, 'The APEC Cross Border Privacy Rules system: A Civil Society perspective' (Privacy International, 6 July 2013) <https://www.privacyinternational.org/blasts/the-apec-cross-border-privacy-rules-system-a-civil-society-perspective>.

[15] *Comments on JOP Recommendation submitted to ECSG Chair, 19 February 2013* (Comments by civil society organisations submitted to JOP by Nigel Waters, 11 March 2013). The authors are two of the civil society representatives that drafted the Comments.

[16] CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013).

[17] It claimed TRUSTe failed to meet APEC requirements at all (13/21), or failed to fully meet them (8/21).

restricted monitoring and certification to online activity (whereas APEC criteria required all activity to be monitored and protected), that it failed to address questions of conflict of interest, was incomplete because some information was withheld as supposedly 'commercial in confidence', and that it proposed to hide APEC case notes or statistics in larger result sets. The JOP's final recommendation of approval[18] required TRUSTe to address some of these criticisms, including monitoring non-online activities, and separating complaint reporting. It did not address the program requirement criticisms except to require TRUSTe to post online its requirements and the JOP approval.

The civil society submissions, in our view, presented a cogent argument to JOP that TRUSTe failed (and continues to fail) to meet APEC requirements to an extent exceeding what JOP and APEC member economies should accept. However, this description of the first AA approval process is also significant because the only reason any of these issues (including those that JOP requires TRUSTe to address) came to light at all, is the coincidence that a civil society representative was part of one of the member economy delegations. There is no external or critical perspective built in to these CBPRs processes, and this first example shows that it is unlikely to be provided by member economies. The TRUSTe approval as an AA puts into question whether a proposed AA application would ever be refused by the JOP, assuming it is supported by the relevant member economy. If that is questionable, then what credibility can the whole CBPRs process have?

### *The first year of certifications: Somewhat incestuous*

To date, five US companies have been certified by TRUSTe as CBPR-compliant (IBM, Merck, Yodlee, Lynda and Workday). No details are available from TRUSTe demonstrating how any of the companies certified comply with APEC requirements. There is no requirement for there to be any opportunities for third party inputs into certification decisions. The responsible officer of the first company to be certified, IBM,[19] described in an interview the certification process and stressed how little work was required on the company's part to obtain certification.[20] Two of those companies, Yodlee and Lynda, have significant business affiliations with TRUSTe, because of investments in each by Accel Partners, and overlapping board memberships.[21] This raises significant questions of the appropriateness of TRUSTe certifying companies that could be regarded as affiliated businesses, or of its capacity to be 'independent' in resolving any disputes between these companies and data subject.

### *The AA renewal process: A test of credibility for JOP*

TRUSTe's approval as an AA was only for one year, to June 2014. Although JOP does not invite external submissions, the Australian Privacy Foundation (APF), on the basis that it is the leading civil society privacy organisation in one APEC economy, has submitted to JOP and ECSG that TRUSTe's recognition as an AA should not be renewed.[22] It argues that TRUSTe has failed to meet APEC CBPRs criteria in four ways: it has not developed APEC-specific program requirements that meet all of the AA Recognition Criteria (listing 9 such criteria not met), despite undertaking to do so; its program still fails to cover offline activity, mobile applications, cloud services etc., as

---

[18] CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013, as amended 18 June 2013).

[19] IBM 'IBM Becomes First Company Certified Under APEC Cross Border Privacy Rules' (IBM, 12 August 2013) <http://www-03.ibm.com/press/us/en/pressrelease/41760.wss> accessed 14 January 2014.

[20] Laura Linkomes 'IBM first to receive APEC's CBPR certification' (2013) 126 *Privacy Laws & Business International Report*, pgs. 17-19.

[21] Australian Privacy Foundation (APF) 'Submission opposing the 2014 renewal of recognition of TRUSTe as a BBPR Accountability Agent (AA) under the APEC Cross Border Privacy Rules (CBPR) System' (13 June 2014). <http://www.privacy.org.au/> The authors are members of the APF International Committee that drafted the submission.

[22] APF Submission

required; it is not managing apparent Conflicts of Interest appropriately, as it is required to do; and it has failed to comply with APEC's documentation and public disclosure requirements for AAs.

The TRUSTe renewal process will be a test of the credibility of the JOP and of CBPRs generally. Non-renewal of TRUSTe's AA status would give the APEC CBPRs an opportunity to start again with AA recognition based upon the better application of APEC CBPRs standards. Otherwise, the first instance of the application of those standards may give rise to suspicions that they are not taken seriously by JOP or by AAs.

## Conclusions: Credibility tested at a number of levels

This article shows that the APEC CBPRs processes, despite the conscientious efforts to improve them by representatives from some economies, are lacking in significant respects. The Final Reports by the JOP lack sufficient independent assessment by JOP of whether an economy's implementation of its laws will in substance deliver what is required by the APEC CBPRs requirements. The first JOP processes to appoint an AA were flawed to an extent which should not have been acceptable to APEC member economies. Partly as a result, the first year's operation of the only existing AA has been carried out in a way which is not compliant with CBPRs requirements. This means that the renewal of that AA's recognition is a major credibility test for JOP.

Discussions have taken place within the APEC ECSG Data Privacy Subgroup on the ability of stakeholders to participate in discussions on AA applications, but it was decided to do nothing and to allow such matters 'to be raised on an ad-hoc basis'.[23] This unwillingness by some APEC economies to invite and utilise outside input is a major contributor to the credibility problems faced by the CBPRs.

*The final article in this series will make an overall assessment of the APEC CBPRs, and consider the outcome of the renewal of TRUSTe's AA status.*

*Correction: In the previous article by Graham Greenleaf 'APEC's Cross-border privacy rules system: A house of cards?' (2014) 128 Privacy Laws &Business International Report, 27-30, item 1 under 'How does APEC CBPRs work' should have stated the JOP does issue Findings Reports on each economy's application (as discussed in the above article). The point being made was the shortcomings of such JOP assessment, but it could be read as implying there was no JOP report.*

[23] APEC ECSG Data Privacy Sub-group, 'Report of the 29th DPS' (Ningbo, China, 18 February 2014).