Privacy groups win changes to APEC CBPR system

Chris Connolly, Graham Greenleaf and Nigel Waters

(2015) 133 *Privacy Laws & Business International Report,* 32-33 (February 2015)

Privacy advocates and civil society representatives have been campaigning for two years for reform of the APEC Cross Border Privacy Rules system (APEC CBPRs). On 27 January 2015, APEC announced significant changes, meeting around 90% of the demands from that campaign.

Advocates had argued that the first implementation of the APEC CBPRs (using TRUSTe as the Accountability Agent (AA) in the United States) had failed to meet basic APEC Privacy Framework requirements, both in relation to TRUSTe's original AA application in 2013[1] and in its 2014 application for renewal of its AA status. The campaign culminated in a submission by a coalition of consumer and privacy groups from across APEC opposing TRUSTe's renewal as an Accountability Agent.[2]

That renewal was due to be made in June 2014, but the decision by APEC was delayed until January 27 2015[3]. Although APEC chose to ultimately approve TRUSTe's continued role as an Accountability Agent (at least for a further 12 months), the decision was accompanied by massive changes and improvements in the APEC CBPRs, including a completely new set of TRUSTe APEC Program Requirements.

Improvements won

The APEC Recognition Criteria for Accountability Agents (AAs) are the link between the APEC Privacy Principles and the 'on the ground' application of those Principles in the CBPRs.

In the initial approval of TRUSTe as an AA, many of these Recognition Criteria were simply ignored. TRUSTe initially used its own existing generic program requirements in its application for AA status. After civil society intervention in early 2013, TRUSTe was forced to develop and publish specific APEC CBPR program requirements. However, these revised TRUSTe program requirements still did not meet key AA Recognition Criteria and APEC Privacy Principles.

---

[1] See Greenleaf, G and Waters, N 'APEC's CBPRs: Two years on – take-up and credibility issues' (2014) 129 *Privacy Laws & Business International Report*, 12-15 <http://ssrn.com/abstract=2481812 >

[2] Joint Civil Society Submission to APEC regarding the CBPR system, 3 December 2014, <http://www.privacy.org.au/Papers/APEC-CBPR-141203.pdf>; see also Connolly, C, Greenleaf, G and Waters N 'Privacy self-regulation in crisis?: TRUSTe's 'deceptive' practices' (2014) 132 *Privacy Laws & Business International Report,* 19-21 < http://ssrn.com/abstract=2567090> .

[3] The recommendation by APEC CBPRs Joint Operations Panel (JOP) was made in late December 2014.

Some key gaps included: there was no 'notice of collection' requirement for any circumstances other than online collection of data (Criterion 2); there was no requirement for collection to be fair (Criterion 7 and APEC Privacy Principle 3); the requirement that access to personal information must be provided within a reasonable time was missing (Criterion 37B); and the requirement that correction should be provided within a reasonable time was missing (Criterion 38C).

Another significant gap in TRUSTe's application relates to the security test. APEC AA Recognition Criteria 30 states that security safeguards have to be 'proportional to sensitivity of information and the probability and severity of the harm'. This is an important provision – it took years to negotiate. It is one of the most high profile provisions of the APEC Privacy Principles (Principle 7) – it is in the core wording of the principle, not just in a footnote. It has even been interpreted by some parties, including the EU, to align with the treatment of 'sensitive data' in other privacy regimes.

However, this provision was completely missing from the TRUSTe APEC requirements. In the initial TRUSTe program requirements the security test said that safeguards were to be proportional to the 'size of the business'. There was no mention of the sensitivity of the data or the severity of the harm.

It should have been a matter of great concern for APEC that the APEC Privacy Principles, which took years to negotiate, and on which the AA criteria are based, had been so comprehensively undermined in their very first implementation. The Framework itself promised that: 'cross border privacy rules should adhere to the APEC Privacy Principles'.

It took three separate attempts over a two year period by privacy and civil society representatives to finally convince APEC to fix this issue. On 27 January 2015 TRUSTe finally published new program requirements that included the APEC security test, rather than their own weaker test.

The new program requirements fixes numerous other gaps, including the introduction of a 'fair collection' test, along with the extension of the program to all personal data collection (rather than the previous restriction to online data collection). Significant omissions in the access and correction provisions were also corrected.

APEC also finally published an accurate list of certified members, including contact details and certification expiry dates.[4] This had been a major part of the civil society campaign, and brings APEC into compliance with its own rules, 18 months after the CBPR system was launched.

APEC's own documentation of its re-approval of TRUSTe makes no mention of the fact that these changes to practices came about through civil society exposure and pressure. The new program requirements are actually the *third* version that has been published by TRUSTe in just 2 years, with significant improvements in each version only being achieved after

[4] See the 'Compliance Directory' now available from <www.cbprs.org>

campaigns by advocates. Unfortunately, the different versions are not dated or numbered, and TRUSTe has removed the two previous versions from their website. However, they are still available via Internet archive searches such as The Wayback Engine.

Continuing deficiences and next steps

This has been an excellent result for consumers after a lengthy campaign. However, three issues that were raised by civil society representatives have only been partially addressed, and there is still room for further improvement of the APEC CBPR system. These issues are:

1. Conflicts of Interest

Civil society representatives complained that TRUSTe was certifying companies where the target company had the same owners and directors as TRUSTe. Although this complaint was found to be partially correct, APEC have decided that TRUSTe has sufficient internal safeguards in place to prevent any conflict of interest occurring. These safeguards include several internal conflict of interest guidelines issued or revised in 2014, although it is unclear whether these guidelines will be made available to the public.

2. False claims

APEC have not directly addressed the issue of false claims of APEC certification (where companies fraudulently claim in their privacy policies that they are APEC CBPRs members), but they did invite civil society organisations to send examples to APEC for unspecified "action". Around 12 examples have been forwarded to APEC and to US regulatory authorities in the last year, although there has been no official response or enforcement action to date. This may not sound like a large number, but there are only 10 *real* APEC certifications at the time of writing.

3. Fine print exclusions

Civil society representatives complained that some APEC CBPRs members use fine print in their privacy policies to exclude certain activities, such as mobile applications and cloud services, from their APEC certification. APEC have concluded that this behaviour is actually allowed under the CBPRs rules. They point out that exactly the same 'scoping' issue occurs in the EU US Safe Harbor. These fine print exclusions are a potential trap for consumers who may see a high profile APEC logo (or a Safe Harbor logo), but would be unlikely to find the fine print exclusions or realise their importance.

Conclusion

Overall this is a big win for consumers. The new TRUSTe program requirements have finally complied with the APEC Privacy Principles and the Accountability Agent recognition criteria. These improvements have been complemented by significant upgrades to both the APEC and TRUSTe websites, so that an accurate list of certified companies, with contact details and expiry dates, is finally available.

These changes are the result of a two year campaign by civil society representatives, and the

TRUSTe program requirements are actually the third version they have issued. None of this is publically acknowledged by either APEC or TRUSTe.

There is always room for improvement in any privacy regulatory or self-regulatory scheme. Following this decision consumers still need to exercise extreme care to avoid false claims of APEC CBPRs certification and also to avoid significant exclusions in the fine print, but many other important issues have now been fixed.

Chris Connolly, Graham Greenleaf and Nigel Waters were involved in the Australian Privacy Foundation's submissions to APEC concerning TRUSTe, and in drafting the Civil Society petition concerning TRUSTe's actions in late 2014.