Australian Privacy Foundation	Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic	Center for Digital Democracy	Electronic Privacy Information Center	Open Net Korea	Privacy International

Urgent call for reform or closure of the APEC Cross Border Privacy Rules (CBPR) system, and non-renewal of TRUSTe's AA status

To: APEC CBPRs JOP, APEC ECSG Chair and APEC Member Economies

3 December 2014 ***[Revised 11 December 2014 to add two supporting members]***

Introduction

The APEC Cross Border Privacy Rules system (APEC CBPRs) has been operating for 18 months. Over 100 individual company websites now claim to be APEC CBPRs compliant in their privacy policies, and the number is growing rapidly.

However, the first implementation of the APEC CBPRs (using TRUSTe as the Accountability Agent (AA) in the United States) has failed to meet even the most basic of APEC's own Privacy Framework requirements:

1. The APEC recognition criteria for AAs have been comprehensively ignored – TRUSTe's program requirements are a weak subset of APEC's own criteria;
2. TRUSTe has been certifying companies that share the same owners and directors as TRUSTe, in an apparent breach of the APEC Conflict of Interest requirements;
3. Companies have been including very extensive exclusions in the fine print of their privacy policies that completely undermine the APEC requirements – including total exclusions for personal information provided in mobile applications, cloud services and 'behind logins';
4. There are already numerous false claims of APEC certification, even after less than 18 months of operation, without any sign of this apparent deception being detected or investigated;
5. There is no authoritative up-to-date list of certified companies, on either the TRUSTe or CBPRs websites. The CBPRs website is still regarded by APEC's Joint Operating Panel (JOP) as a temporary 'stop-gap' measure, and it maintains a different list than that maintained by TRUSTe. Both lists will mislead consumers as they are both incomplete, and the inconsistency

adds to the confusion; and

6. APEC has failed to publish on the CBPRs website renewal or expiry dates for the annual certification of each company. This will also mislead consumers.

Privacy and consumer civil society representatives now call on APEC to urgently reform the operation of the APEC CBPRs and to put proper resources and infrastructure in place to ensure that the system is administered and enforced in accordance with the APEC requirements. Civil Society organisations have already brought all of these matters to the attention of APEC CBPRs, and it has failed to act upon them. TRUSTe's required 'annual' renewal of its AA status is now nearly half a year overdue.

We also call on APEC to open up key aspects of the APEC CBPRs to proper consultation with stakeholders, including civil society representatives.

APEC recognition criteria for Accountability Agents

The APEC recognition criteria for Accountability Agents (AAs)[1] have been consistently ignored both by APEC and by the only AA appointed to date (TRUSTe) – TRUSTe's program requirements are a weak subset of the APEC criteria.

After civil society intervention, TRUSTe was forced to develop and publish specific APEC CBPR program requirements. These are available at:
http://www.truste.com/privacy-program-requirements/apec

However, these revised TRUSTe program requirements do not meet key AA Recognition Criteria. For example:

- There is no "notice of collection" requirement for any circumstances other than online collection of data (Criteria 2);
- There is no requirement for collection to be *fair* (Criteria 7);
- The requirement for correction of inaccurate data to be forwarded to agents and relevant third parties is missing (Criteria 23 and 24);
- The requirement that agents and third parties must inform the organisation regarding inaccurate data is missing (Criteria 25);
- APEC states that security safeguards have to be "proportional to sensitivity of information and the probability and severity of the harm". The TRUSTe test says that safeguards are to be proportional to "size of the business". This is a completely different test. (Criteria 30);
- The requirement that access to personal information must be provided within a reasonable time is missing (Criteria 37B);

[1] Available at:
https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Application%20for%20APEC%20Recognition.pdf

- The requirement that correction should be provided within a reasonable time is missing (Criteria 38C); and

- The restriction on third parties undertaking further sub-contracting without consent is missing (Criteria 47).

It should be a matter of great concern for APEC that the APEC Privacy Principles, which took years to negotiate, have been completely undermined in their very first implementation. APEC must insist on basic compliance with the recognition criteria by all applicants for AA status.

Conflicts of Interest

TRUSTe has been certifying companies that share the same owners and directors as TRUSTe in an apparent breach of the APEC Conflict of Interest requirements.

Civil Society representatives warned APEC in 2013 that conflicts of interest would be a major issue for TRUSTe, and civil society submitted that APEC should not recognise TRUSTe as an AA without investigating whether TRUSTe had shared ownership and control with the organisations that it certifies. These concerns were completely ignored.

As a result, even though only a small number of companies have been certified in the APEC CBPR system, two of them already have a very significant business affiliation with TRUSTe. TRUSTe shares the same major owners with Yodlee.com and Lynda.com, and even shares a common Director with Lynda.com.

This is a situation that is unthinkable in other jurisdictions, where privacy is regulated by independent entities, and where disputes are heard by organisations that are required to apply very strict rules on independence.

The APEC CBPRs documents purport to include strict requirements regarding conflict of interest, including a prohibition on any actual or potential conflict. The recognition criteria specifically state that an organisation "must not act as an Accountability Agent for a related entity". Examples include "where officers of the applicant entity serve on your organisation's board of directors in a voting capacity (and vice versa)".

It is difficult to see how TRUSTe is in compliance with these very clear requirements.

It is also important to note that TRUSTe has recently reached a draft settlement with the Federal Trade Commission regarding public statements made by TRUSTe and TRUSTe certified companies. This settlement is the result of a six year campaign by consumer and privacy advocates, and an eighteen month formal complaint period with the FTC.

Although the settlement will not be finalised until the current 30 day public consultation period is complete, the proposed consent order[2] prohibits TRUSTe from making any further false or misleading claims regarding "the corporate status of Respondent [TRUSTe] and its independence" (emphasis added). The prohibition also applies to organisations certified by TRUSTe.

[2] The proposed consent order is dated 17 November 2014 and is available at:

When this consent order is finalised, the requirement for TRUSTe not to mislead consumers about its "independence" will be binding on TRUSTe for 20 years, and any breach will trigger civil penalties. TRUSTe will also be required to pay a $200,000 fine for its misleading and deceptive conduct between 2007 and 2013.

This FTC enforcement action and sanction was only made possible by the efforts of the same privacy and consumer advocates who have been warning APEC about TRUSTe since 2009, and the FTC investigation is based in part on the same information supplied to APEC by civil society representatives opposing TRUSTe's initial accreditation as an AA.

Exclusions

Companies certified by TRUSTe have been including very extensive exclusions in the fine print of their privacy policies that completely undermine the APEC requirements – including total exclusions for personal information provided in mobile applications, cloud services and 'behind logins'.

For example, the Yodlee Privacy Policy states: "The TRUSTe program covers only information that is collected through these Web sites … and does not cover information that may be collected through any mobile applications or downloadable software". On some Yodlee websites the privacy policy also specifically excludes TRUSTe coverage of anything "behind the log in of this website". That is exactly where the majority of personal information is likely to be held.

There are numerous other examples. For instance, the IBM Privacy Policy states: "The TRUSTe program does **not** cover information that may be collected through downloadable software, SaaS offerings, or mobile applications." The Merck Online Privacy Policy states: "This policy does **not** apply to personal information collected from offline resources and communications."

All of this is an apparent breach of the APEC CBPRs which requires comprehensive coverage of all personal information collected from any source.[3] It will result in consumers being misled by all of these companies because consumers will understandably assume, based on the APEC requirements, that TRUSTe's 'APEC certification' of each company applies to all personal information collected by the company. In fact, it will apply to very little of the information collected by these companies.

False claims of APEC certification

There are already numerous false claims of APEC certification, even after only 18 months of operation, without any sign of this deceptive and potentially fraudulent conduct being detected or investigated by APEC.

Claims of compliance with APEC CBPRs are springing up in the privacy policies of US companies that are not listed on either the APEC site or the TRUSTe site. Sites like maxmiro.com, www.goldcoastintimates.com, beker-jonze.com and broadbandinhand.com all claim to be APEC CBPRs compliant. There are more, and the number of false claims is growing rapidly. At the time of writing,

---

http://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf

[3] See Paragraph 8 in Policies Rules and Guidelines at: https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20-%20Policies,%20Rules%20and%20Guidelines%20.pdf

there are more false claims than real claims of APEC CBPRs membership.

There are no resources or infrastructure in place in the APEC CBPRs system, by JOP or by the FTC as the USA's APEC enforcement agency, to detect this type of deception, and there are no measures in place to prevent it occurring again and again. TRUSTe could, but does not, take its own steps to counter such abuse of the system that it administers for the USA. It is important to remember that the EU US Safe Harbor began with just a few scattered cases of false claims, but through lack of resources and lack of enforcement this grew to over 850 false claims being reported in 2013/2014 to the FTC. It is now a matter of urgency that both APEC (through its CBPRs JOP) and the FTC start to take rigorous punitive steps against these companies, and announce publicly that they are doing so.

The list of certified companies

After 18 months of operation, and numerous requests, there is still no authoritative list of certified companies available. A temporary list described as a 'stopgap' by APEC was finally provided in late 2014 at cbprs.org, but it is constantly out of date and it is not 'synced' to the list of APEC privacy seals maintained by TRUSTe. At the time of writing it is clearly incorrect, as it lists fewer organisations than the list provided by TRUSTe.

The list at cbprs.org does not provide any contact information – not even the URL of the certified company.

TRUSTe provides their own list of certified companies, but this list is also constantly out of date. It doesn't even include companies who have issued major press releases announcing their TRUSTe APEC certification – even when these press releases are issued by TRUSTe itself (see, for example, box.com). Again, the list does not provide any contact information – it is just a column of company logos.

The APEC CBPR Framework states:

> APEC Economies will establish a publicly accessible directory of organizations that have been certified by Accountability Agents as compliant with the CBPR System. The directory will include contact point information that consumers can use to contact participating organizations. Each organization's listing will include the contact point information for the APEC-recognized Accountability Agent that certified the organization and the relevant Privacy Enforcement Authority. Contact point information allows consumers or other interested parties to direct questions and complaints to the appropriate contact point in an organization or to the relevant Accountability Agent, or if necessary, to contact the relevant Privacy Enforcement Authority.

APEC have been describing the site as 'temporary' or 'stop-gap' for the entire period of operation of the CBPRs, and APEC's JOP claims that it is difficult to keep its website consistent with that of TRUSTe without stating what steps it is taking to do so. Consumers deserve a better source of official, up to date information, and are likely to be misled if one does not exist. APEC's JOP is fully aware that consumers are being misled because of the failure to keep the APEC website up-to-date, and the failure of TRUSTe to publish an accurate list and contact details of companies that it has certified. It appears that the APEC system as a whole is incapable of being administered as it is required to be, placing customer privacy at risk.

Expiry dates

APEC has failed to publish renewal or expiry dates for the annual certification of each company.

Now that the CBPRs is more than 12 months old, the certifications of companies will begin to expire. They are supposed to be renewed annually, but the renewal dates for particular companies will be scattered throughout the year.

Despite repeated requests neither APEC or TRUSTe have published expiry and renewal dates. This has been one of the most persistent problems in other privacy self-regulatory schemes, particularly the EU US Safe Harbor. Earlier this year, following complaints by consumer and privacy advocates, the FTC finally took action against companies who had been pretending to be Safe Harbor members up to 8 years after their membership expired (several of the companies had been certified by TRUSTe).[4] This action was only possible because the expiry dates were made public by the Department of Commerce.

In addition, the FTC has finally taken action against TRUSTe (after a six year campaign and an 18 month formal complaint period) regarding its failure to conduct annual re-certifications in key schemes such as the EU US Safe Harbor and the COPPA Safe Harbor.[5] The FTC found that in over 1,000 cases annual re-certifications were not conducted, and TRUSTe still allowed companies to display a TRUSTe seal, even in programs with a strict requirement for annual verification (such as the EU US Safe Harbor). This complaint by privacy and consumer advocates has led to a proposed $200,000 fine for TRUSTe and a range of other sanctions. This case demonstrates the importance of publishing renewal and expiry dates, and taking steps to ensure that annual re-certifications are being conducted in accordance with the APEC CBPRs requirements.

TRUSTe has now admitted that annual re-certifications did not occur in up to 10% of cases between 2007 and 2013.[6] No such admission was made in TRUSTe's application to APEC for AA accreditation in 2013, or their application for renewal in 2014.

APEC's JOP is fully aware that key information on renewal and expiry dates has been withheld from consumers, as a result of submissions made by the Australian Privacy Foundation.

Process Issues

APEC has taken nearly 6 months to consider the renewal of TRUSTe's accreditation in the light of important civil society submissions. There is no formal APEC CBPRs process for stakeholder consultation regarding these renewals, and APEC has not sought any input.

While various APEC governments have been open to civil society input, APEC has rejected formal and direct civil society representation in any of its processes for developing and implementing the APEC Privacy Framework. This has prevented the APEC CBPRs from reflecting civil society concerns in a

[4] See: http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply

[5] See: http://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its

[6] See the TRUSTe blog entry regarding the FTC settlement at: http://www.truste.com/blog/2014/11/17/truste-ftc/?utm_source=rss&utm_medium=rss&utm_campaign=truste-ftc

meaningful way and, by extension, to the many problems highlighted above.

Privacy and consumer civil society representatives now call on APEC to open up key aspects of the APEC CBPRs to proper consultation with stakeholders, including civil society representatives.

Conclusion

The civil society representatives that have signed this letter call on APEC to take urgent steps to reform the APEC CBPRs, and to put in place proper resources and infrastructure to ensure that the system is administered and enforced in accordance with the APEC requirements. Alternatively, the whole CBPRs system should be closed down before it does further harm to consumers.

The current implementation does not comply with the basic AA Recognition Criteria. The organisations that have been certified are riddled with conflicts of interest, fine print and exclusions that undermine the APEC Privacy Framework. There is no infrastructure in place to provide up to date information, contact details and renewal / expiry dates for certified companies, and the whole scheme has already been infiltrated by numerous false claims of APEC certification, without any detection or enforcement action.

Civil Society organisations therefore call upon APEC to refuse to renew the AA status of TRUSTe. Civil Society organisations also call upon APEC to refer the clear breaches of US law by some US companies that are making false claims to the US Federal Trade Commission (FTC), because there is no possibility (based on its past conduct) that TRUSTe will do so.

In short, the current implementation of the APEC CBPRs is doing more harm than good and needs very urgent and extensive reform or to be disbanded.

We look forward to your response.

Yours sincerely,

Chris Connolly, Chair, International Committee	**Tamir Israel, Staff Lawyer**	**Jeff Chester, Executive Director**	**Marc Rotenburg, President and Executive Director**	**K.S. Park, Director**	**Gus Hosein, Executive Director**
Australian Privacy Foundation	**Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic**	**Center for Digital Democracy**	**Electronic Privacy Information Center**	**Open Net Korea**	**Privacy International**
www.privacy.org.au	www.cippic.ca	www.democraticmedia.org	www.epic.org	www.opennetkorea.org	www.privacyinternational.org

Correspondence can be directed to:

Chris Connolly
chrisc@galexia.com