Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

Submission opposing the 2014 renewal of recognition of TRUSTe as a CBPR Accountability Agent (AA) under the APEC Cross Border Privacy Rules (CBPR) system

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

From: Australian Privacy Foundation, International Committee

13 June 2014

Introduction

On June 25 2013 TRUSTe was recognised as the first APEC CBPR Accountability Agent (AA). This decision was made in spite of evidence presented to APEC that TRUSTe's application for recognition did not meet the required AA Recognition Criteria.

The recognition of TRUSTe as an AA is now due for renewal by 30 June 2014.

The Australian Privacy Foundation (APF), via its International Committee[**], is making this formal submission opposing the renewal of the recognition of TRUSTe as a CBPR Accountability Agent (AA). Australia is an APEC Member Economy, and a potential participant in the APEC CBPRs. The APF is Australia's only non-government organisation dedicated to privacy advocacy, operating since 1987. Background on the APF is available at www.privacy.org.au.

There is no formal APEC CBPRs process for consultation regarding these renewals, and APEC has not sought any input. However, the APF is making this submission in the expectation that serious deficiencies in TRUSTe's processes will be addressed by the JOP and ECSG.

APF submits that TRUSTe continues to breach the Recognition Criteria. Many of the issues and warnings that civil society representatives raised during the rushed JOP process to recognise TRUSTe

[**] The members of the International Committee include Chris Connolly (Chair), Nigel Waters, Prof Roger Clarke (APF Chair), Prof Dan Svantesson, Prof Graham Greenleaf, David Vaile and Prof Lee Bygrave.

in 2013 have now come true in practice. APEC Member Economies should be very concerned about the potential damage being done to the APEC Privacy Framework. APF submit that TRUSTe's recognition as an AA should not be renewed, on four grounds:

(i) TRUSTe has not developed APEC specific program requirements that meet all of the AA Recognition Criteria, despite undertaking to do so;

(ii) The TRUSTe program still fails to cover offline activity, mobile applications, cloud services etc., in breach of APEC CBPRs requirements;

(iii) TRUSTe is not managing Conflicts of Interest appropriately, in breach of APEC CBPRs requirements; and

(iv) TRUSTe has failed to comply with the documentation and public disclosure requirements in the AA Recognition Criteria.

Non-renewal of TRUSTe's AA status will give the APEC CBPRs an opportunity to start again with AA recognition based upon the better application of APEC CBPRs standards, without the first instance of the application of those standards demonstrating that they are not taken seriously by JOP or by AAs.

(i) TRUSTe has not developed APEC specific program requirements that meet all of the AA Recognition Criteria, despite undertaking to do so

At the time of its application, TRUSTe did not have specific APEC CBPR program requirements. Civil society submissions (CS submissions) warned APEC member economies that TRUSTe should not be recognised until they submitted specific APEC Program Requirements. CS submissions provided evidence that TRUSTe was merely relying on its existing Website Privacy Seal program requirements in their AA application.

The JOP final decision (only after civil society intervention) stated that TRUSTe had promised to develop and publish specific APEC CBPR program requirements that met the Recognition Criteria.

These have now been made available at:

http://www.truste.com/privacy-program-requirements/apec

We note that TRUSTe has amended the requirements to address some of the issues raised by civil society representatives. These include:

- A new requirement for complaints to be dealt with in a 'timely' manner as required by AA Recognition Criteria 42;
- The replacement of all references to 'commercially reasonable' with the APEC agreed term 'reasonable';
- The introduction of a new section on training, as required by AA Recognition Criteria 44; and
- The introduction of a new data breach notification requirement, as required by AA Recognition Criteria 35 and 47.

These important changes would not have occurred without the intervention of civil society representatives, as the original JOP recommendation ignored these missing requirements, and no APEC Member Economy raised these issues.

Despite these changes, the revised TRUSTe program requirements still do not meet key AA Recognition Criteria. For example:

- There is still no "notice of collection" requirement for any circumstances other than online collection of data (Criteria 2);

- There is still no requirement for collection to be both lawful and *fair*. If fair collection is an APEC requirement then an AA approved by APEC should take some responsibility for ensuring compliance with fair collection. APEC has spent years developing a framework, principles, CBPR rules and AA criteria that all require 'fair collection'. This simple but important test is still missing from TRUSTe's APEC CBPR program requirements (Criteria 7);

- The requirement for correction of inaccurate data to be forwarded to agents and relevant third parties is still not a TRUSTe program requirement. The APEC requirement requires forwarding of corrections AFTER they are discovered, at any time. The TRUSTe requirement is still limited to accuracy "in the first instance" (Criteria 23 and 24);

- The requirement that agents and third parties must inform the organisation regarding inaccurate data is still not a TRUSTe program requirement. When CS submissions raised this gap the JOP replied that "Section III.E.A of TRUSTe's program requirements requires steps by the participant to ensure data received from third parties is accurate and requires any third party to report incorrect data to the participant such that the participant is then able to conform to the requirements in this section." CS submissions have pointed out previously that there is no Section III.E.A in the TRUSTe program requirements. It does not exist. There still do not appear to be any requirements that meet this specific APEC test (Criteria 25);

- APEC Criteria 30 states that "Safeguards have to be proportional to (1) sensitivity of information; and (2) the probability and severity of the harm". The TRUSTe test still says that safeguards are to be proportional to 'size of the business'. This is a completely different test. The 'size of the business' should not be a criteria in this APEC specific program – it may be part of TRUSTe's approach in other areas, but it needs to be specifically ruled out as a criteria in APEC. APEC Member economies have NOT agreed to approve privacy compliance arrangements which have a different test depending on the size of the business. A tiny business could have an enormous impact on privacy (Criteria 30).

- APEC requires access to be provided within a reasonable time – TRUSTe still does not include this requirement in their APEC program requirements. When civil society submissions raised this issue previously, the JOP pointed to TRUSTe program requirements at IV.A.1.a-b. This is a serious error. CS submissions have already notified APEC that the main TRUSTe program does not include *any* timeline or *any* requirement for a timely response to access requests. The IV A.1 requirements ONLY apply to EU Safe Harbor members. Obviously not all TRUSTe APEC CBPR members will be Safe Harbor members. This is a very serious and straight forward error that the JOP and TRUSTe have failed to rectify despite several opportunities. (Criteria 37B)

- The APEC requirement that correction should be provided within a reasonable time is still not a TRUSTe program requirement. Again, this is a very simple requirement. How will TRUSTe clients even know that this APEC requirement exists if it is not included in the program rules? (Criteria 38C).

- APEC requires restrictions on third parties undertaking further sub-contracting without consent. This is still not a TRUSTe program requirement (Criteria 47).

(ii) The TRUSTe program still fails to cover offline activity, mobile applications, cloud services etc., in breach of APEC CBPRs requirements

TRUSTe has failed to address one of the key concerns raised in the CS submissions. It still only applies its APEC CBPR certification (and dispute resolution services) to online activities related specifically to the organisation's website. TRUSTe still excludes protection for consumers who interact with the organisation offline, or through mobile apps, downloaded software, cloud services or any other channel.

Since earlier CS submissions, TRUSTe has added one short clause to the APEC program requirements:

> "I. Scope
>
> The APEC Privacy Program is designed for businesses collecting personally identifiable information directly from consumers and transferring that information between economies within the APAC (sic) region participating in the Cross Border Privacy Rules (CBPR) Framework. This program certifies both online and offline data collection practices of businesses as being in compliance with the CBPR Framework."

Once again, even this short clause would not have been added without the important intervention of civil society representatives, as the original JOP recommendation completely ignored this issue.

However, although the new clause purports to extend TRUSTe's certification to offline data collection and other forms of data collection, the rest of the program requirements are ONLY concerned with online data collection, and there is no other reference to offline data in the entire set of requirements.

See for example:

- "All Participants wanting to be certified that their Online information collection and use practices comply with TRUSTe's Privacy Program Requirements must comply with the following requirements:" (Minimum Program Requirements)

- "A. Provide, at no charge to TRUSTe or its representatives, full access to the Online properties (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices. B. Provide, upon TRUSTe's reasonable request, information regarding how PII gathered from and/or tracked through Participant's Online properties is used." (Accountability)

- "Participant's material failure to permit or cooperate with a TRUSTe investigation or review of Participant's Online properties or practices pursuant to the Program Requirements" (Termination)

- "Information collected by the Participant or the Participant's Service Provider may be used to tailor the Individual's experience on the Participant's Online property." (Use of PII)

More importantly, TRUSTe has specifically and severely restricted the scope of its certification in four of the five instances where it has certified a US company as a member of the APEC CBPR program.

For example:

- The Yodlee Privacy Policy states: "The TRUSTe program covers only information that is collected through these Web sites: (www.yodlee.com plus a list of related sites) and does not cover information that may be collected through any mobile applications or downloadable software." On some of the key listed websites, such as www.moneycenter.yodlee.com, the privacy policy also specifically excludes TRUSTe coverage of anything "behind the log in of this website".

- The IBM Privacy Policy states: "The TRUSTe program covers only information that is collected through www.ibm.com and does not cover information that may be collected through downloadable software, SaaS offerings, or mobile applications." IBM has a completely separate privacy policy for cloud and software services that does not mention APEC at all.

- The Merck Online Privacy Policy states: "This policy applies to personal information (as defined below) collected from Merck online resources and communications (such as Web sites, e-mail, and other online and downloadable tools) that display a link to this policy. This policy does **not** apply to personal information collected from offline resources and communications, except in cases where such personal information is consolidated with personal information collected by Merck online."

The following table summarises compliance with the APEC CBPR requirement that all data is covered by the AA's certification.

Participant	Compliance	APEC CBPR should apply to *all* personal data
TRUSTe (AA)	No	The TRUSTe APEC program requirements have one short clause stating that they apply to offline data, but the rest of the requirements only discuss online data.
IBM	No	The IBM Privacy Policy specifically excludes cloud and software services from its TRUSTe certification, even though these are their most high profile services.

Participant	Compliance	APEC CBPR should apply to *all* personal data
Merck	No	The Merck Privacy Policy specifically excludes offline activity.
Yodlee	No	The Yodlee Privacy Policy specifically excludes mobile applications and downloadable software, even though these are a major part of their service offering. Some Yodlee sites also exclude any activity behind the login.
Lynda	Yes	Comprehensive coverage
Workday	No	The Workday Privacy Policy specifically excludes "information that may be collected through our applications", even though these are a major part of their service.

Civil Society submissions warned APEC that this would be one of the biggest issues if TRUSTe was approved as an AA. When an organisation is bound by privacy legislation it is typically bound for *all* of its personal data. That is not how TRUSTe operates. They have multiple small programs for numerous categories of data. They go to great lengths to exclude certification, coverage, dispute resolution and protection for any categories that an organisation has not subscribed to.

CS submissions previously warned APEC that there is a long history of complaints and case law in which TRUSTe refused to offer protection because data was collected by downloadable software, or in a members-only login area. These warnings were ignored and APEC now has four US companies branded as APEC CBPR members where consumers have no recourse in relation to their most popular services, such as mobile apps, cloud services, member services and offline services.

Consumers reading these privacy policies will be given the misleading and false impression that the APEC CBPR requirements only apply to a small fraction of the data collected by these companies.

In addition, as stated in previous CS submissions, the compliance monitoring tools used by TRUSTe only apply to online activity, such as their web-crawling tool and email seeding.

(iii) TRUSTe is not managing Conflicts of Interest appropriately, in breach of APEC CBPRs requirements

The earlier CS submissions warned 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.

The response by the JOP did not expressly address the Recognition Criteria sections that deal with **business affiliations**. CS submissions warned that it is not clear how TRUSTe would deal with the situation of applications for certification from businesses which have a shared commercial link with TRUSTe (or of complaints about such businesses if certified). The JOP did not address the issue of public perceptions or public concerns about conflicts of interest in these situations. In general the JOP report avoided these issues.

APEC is now going to have to face these difficult issues. Even though only five companies have been certified in the APEC CBPR system, two of them already have a very significant business affiliation with TRUSTe.

Yodlee is an account aggregation provider. Yodlee's largest owner, investor and controller is Accel Partners, who are reported to have invested as much as $100 million USD in the company. Naturally they are represented on the Board of Directors of Yodlee.

Lynda.com is an online training services provider. Their largest owner, investor and controller is also Accel Partners, who are reported to have led a consortium of investors in providing over $100 million USD for Lynda.com in 2013. Naturally they are represented on the Board of Directors of Lynda.com.

Accel Partners are also the largest owner, investor and controller of TRUSTe. Accel Partners have one director on the (small) TRUSTe Board of Directors. In any APEC member economy these three organisations would be categorised as affiliated businesses.

Further, one member of the TRUSTe Board of Directors from Accel Partners (Andrew Braccia) is also reported by Accel Partners, Businessweek and other corporate news sites to have been appointed as a member of the Board of Directors of Lynda.com in 2013.

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 subject to very strict rules on independence.

The public, not to mention European and other non-APEC regulators, will be justified in questioning whether one organisation should be able to certify another organisation with such a clear level of shared ownership and control. No matter what documentation and separation is in place within TRUSTe, this situation should never have been allowed to arise. APEC is now putting its name and reputation to this outcome.

CS submissions also warned that organisations certified by TRUSTe always include a statement that TRUSTe is an "independent" third party. Despite the shared ownership and control, the Yodlee privacy policy and the Lynda.com Privacy Policy both include this claim of 'independence', and there is no disclosure of the link between these companies.

Interestingly, Accel Partners does not make any such claims of independence. It lists the three companies (TRUSTe, Yodlee and Lynda) as "**our** companies".

The conflict of interest issue is so important that APF submits that TRUSTe (and any other AA applicant in future) should be required to exclude any affiliated businesses from their APEC CBPR system.

The current APEC CBPR website also includes a statement on the purported *ongoing* conflict of interest requirements for AAs. It states:

> **No actual or potential conflict of interest**
>
> An Accountability Agent must have no actual or potential conflict of interest. Your organisation must not act as an Accountability Agent for a related entity or where there is a risk that your organisation's professional judgement, integrity and/or objectivity could be influenced by the relationship with that entity.
>
> Where your organisation considers that it can continue to act where a potential conflict of interest has arisen (e.g. due to internal safeguards), your organisation must promptly notify the Joint Oversight Panel of the potential conflict of interest and explain how the organisation will ensure that the circumstances will not compromise your organisation's ability to make a fair decision.
>
> Examples of situations where notification is required:
>
> •officers of the applicant entity serve on your organisation's board of directors in a voting capacity (and vice versa);
>
> •officers of the entity that your organisation has certified serve on your organisation's board of directors in a voting capacity (and vice versa);
>
> •there is a commercial relationship between your organisation and the entity applying for certification or the entity that has been certified by your organisation;
>
> •your organisation has entered into significant monetary arrangement with the entity applying for certification or the entity that has been certified by your organisation.
>
> Please note: If the Joint Oversight Panel is not satisfied that the potential conflict of interest can be averted, it will ask your organisation to withdraw from the engagement.

It is impossible to understand how TRUSTe is in compliance with these very clear requirements.

(iv) TRUSTe has failed to comply with the documentation and public disclosure requirements in the AA Recognition Criteria

The formal agreement recognising TRUSTe as an AA requires them to publish their application and attachments on the TRUSTe website. No such documents can be found on the TRUSTe site.

TRUSTe has also failed to provide accurate information regarding the exact websites that it has certified as members of the APEC CBPR system.

APEC member economies may be surprised to learn that dozens and dozens of web sites are listed under the TRUSTe APEC Privacy Seal. For example if you review the TRUSTe verification pages for the five companies that have been certified to date, TRUSTe purports to extend the APEC certification to 54 individual websites.

If you use the TRUSTe "trusted companies" search engine, a range of additional sites are said to be covered by the TRUSTe APEC seal.

The companies themselves purport to extend their privacy policies to cover another 9 websites.

There is absolutely no consistency between the three claims (the TRUSTe verification page, the TRUSTe search engine, and the websites themselves). For example if you follow the links from the TRUSTe verification page for Merck to sites like "MyVetOnline" you will find no mention of APEC, and their privacy policy does not include the required statement that they are complying with the APEC CBPR system.

There are many more examples. This happens because these companies are affiliated with IBM, Merck, Yodlee, Lynda or Workday, but for whatever reason they have not all adopted the central privacy policies of those companies (which do mention APEC).

In all, TRUSTe lists more than 60 websites as members of the TRUSTe APEC program in either its verification pages or search engines. Many of these don't mention APEC and some are broken links or not available.

This is typical of the problems that have beset trustmark sites when they deal with privacy frameworks like the EU / US Safe Harbor. There is no consistency between the claims made by TRUSTe and the claims made by the websites themselves. At least in the Safe Harbor each website can be checked against an **official** list maintained by the US Department of Commerce. In APEC no such list exists. The official CBPR website purports to provide consumers with a list of members, but the link currently leads to the wrong information.

This is despite the APEC CBPR Framework requirement stating:

> 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.

In addition, neither TRUSTe nor the five CBPR members list any information on the date of their recognition or the date of their next renewal. In future years this will undoubtedly become a major problem for the CBPR system, just as it has become a major problem for the EU /US Safe Harbor. Again, the date of recognition and renewal should be listed on the formal APEC CBPR site.