Privacy self-regulation in crisis?
TRUSTe's 'deceptive' practices

Chris Connolly, Graham Greenleaf and Nigel Waters*

(2014) 132 *Privacy Laws & Business International Report*, 13-17, December 2014

Contents

* 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. Thanks to Tamir Israel for valuable comments. Responsibility for content remains with the authors.

A credibility crisis

TRUSTe Inc. is the largest global provider of privacy certifications - 'privacy seals' - to businesses, with the ostensible purpose of assuring consumers that they can have confidence in the privacy practices of those businesses. Its operations in three of the most important (and government-endorsed) privacy self-regulatory schemes in the world have been shown to involve systemic practices which are liable to deceive or mislead consumers concerning the real practices of the companies concerned. These practices occur in self-regulatory schemes affecting the USA (COPPA, the Children's Online Privacy Protection Act), Europe (the EU-US Safe Harbor Framework), and across the whole Asia-Pacific (the APEC Cross-border Privacy Rules System, APEC CBPRs).

The Safe Harbor program is currently under review by the European Union, with many influential European voices calling for it to be terminated, and the European Commission demanding major reforms such as the right for Europeans to sue for breaches in US courts. In November 2014, the US Federal Trade Commission held in a draft consent agreement that TRUSTe had deceived consumers and perpetuated misrepresentations in relation to COPPA and Safe Harbor, imposing a US$200,000 'disgorgement' (giving up profits wrongfully obtained[1]) and other penalties. This enforcement action was the result of a long campaign by privacy advocates, and many of the issues raised in the complaint relate to behaviour by TRUSTe that was first identified in 2009.

Privacy advocates have also been campaigning against TRUSTe's status as the only Accountability Agent (AA) for the USA under the APEC CBPRs. An initial complaint by the Australian Privacy Foundation (APF) in February 2013,[2] was followed by criticism of the initial decision by civil society organisations in April 2013,[3] and by an APF submission opposing re-accreditation of TRUSTe as an AA in June 2014.[4] These have now been followed by a submission to APEC CBPRs from a coalition of civil society organisations from APEC countries demanding that APEC reform its CBPRs or close it down, and that it suspend TRUSTe from the scheme.[5]

---

[1] 'A remedy requiring a party who profits from illegal or wrongful acts to give up any profits he or she made as a result of his or her illegal or wrongful conduct. The purpose of this remedy is to prevent unjust enrichment.' WEX on LII (Cornell) < http://www.law.cornell.edu/wex/disgorgement>.

[2] N Waters (for APF) '(Submission on) Application from TRUSTe for recognition as a CBPR Accountability Agent (AA)' (11 March 2013) <http://www.privacy.org.au/Papers/JOP-TRUSTe-130311.pdf>

[3] N Waters (for APF and CIPIC, Canada) 'Civil Society Comments on the Joint Oversight Panel (JOP) 'Addendum' (April 2013)' (8 May 2013) <http://www.privacy.org.au/Papers/JOP_CivSoc-130508.pdf>

[4] APF 'Submission opposing the 2014 renewal of recognition of TRUSTe as a CBPR Accountability Agent (AA) under the APEC Cross Border Privacy Rules (CBPR) system" <http://www.privacy.org.au/Papers/APEC-CBPR-140613.pdf>

[5] Australian Privacy Foundation (APF), Electronic Privacy Information Centre (EPIC), Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), and the Centre for Digital Democrary (CDC) , Open Net Korea and Privacy International (PI) submission to APEC CBPRs Joint Oversight Committee (JOP),

TRUSTe is therefore under attack on all fronts, and self-regulation of privacy has a global crisis of credibility, affecting also the governments and official bodies operating and promoting these schemes.

The FTC finds TRUSTe 'deceived consumers'

In November 2014, TRUSTe reached a draft settlement with the US Federal Trade Commission (FTC) regarding public statements made by TRUSTe and TRUSTe-certified companies. According to the proposed consent order,[6] TRUSTe will be required to pay a $200,000 fine for its misleading and deceptive conduct between 2007 and 2013, plus a range of other sanctions, because of its failure to conduct annual re-certifications in key schemes such as the EU-US Safe Harbor and the COPPA Safe Harbor,[7] and other breaches of those schemes. FTC Chairwoman Edith Ramirez summed up the FTC's findings as 'TRUSTe promised to hold companies accountable for protecting consumer privacy, but it fell short of that pledge.'[8] The settlement will not be finalised until the current 30 day public consultation period is complete. Each element of the FTC findings is now examined. This case also has implications for APEC CBPRs, as discussed later in this article.

Pretence of Safe Harbor membership

As background to this case, pretence of continuing privacy seal scheme membership after membership had expired has been one of the most persistent problems in privacy self-regulatory schemes, particularly EU-US Safe Harbor. Earlier in 2014, 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.[9] Several of the companies had been certified by TRUSTe. This action was only possible because the expiry dates were made public by the Department of Commerce. Similar issues have arisen in the FTC's current action against TRUSTe, and in relation to the APEC CBPRs.

APEC ECSG Chair and APEC Member Economies, 3 December 2014 'Urgent call for reform or closure of the APEC Cross Border Privacy Rules (CBPR) system, and non-renewal of TRUSTe's AA status' <http://www.privacy.org.au/Papers/APEC-CBPR-141203.pdf>.

[6] *In the Matter of True Ultimate Standards Everywhere, Inc., a corporation d/b/a TRUSTe, Inc. – Agreement Containing Consent Order* (Federal Trade Commission, 17 November 2014) <http://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf >.

[7] FTC 'TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program – Company Failed to Conduct Annual Recertifications, Facilitated Misrepresentation as Non-Profit' (Media Release, 17 November 2014) <http://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.

[8] FTC Media Release, 17 November 2014.

[9] FTC 'FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework' (21 January 2014) <http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply>.

Failure to re-certify companies

In the most recent enforcement action, the FTC found that TRUSTe had represented that it recertified annually all companies displaying a TRUSTe seal, and had done so since 2007. It found that, during that time, in over 1,000 cases annual re-certifications were not conducted, but TRUSTe still allowed the companies to display a TRUSTe seal, even in programs with a strict requirement for annual verification (such as the EU-US Safe Harbor). Therefore, its representations were false and misleading. The proposed consent order requires that TRUSTe shall not make misleading statements about the steps it takes 'to evaluate, certify, review or recertify a company's privacy policies' or the frequency with which it conducts such steps (including recertification). This also prevents it making such statement 'through … licencees' (ie seal holders). Such a prohibition would seem to apply, in future, to misrepresentations about APEC CBPRs recertification. Breach could result in penalties under the FTC legislation. This prohibition does however only apply to misrepresentations, it does not compel TRUSTe to take recertification actions.

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

False claims of non-profit status

The proposed consent order prohibits TRUSTe from making any further false or misleading claims, via its licencees, that it is still a non-profit organisation, when that has been untrue since 2008.[11] This enforcement action is the final step in a long and difficult campaign by privacy advocates to have false claims of TRUSTe's corporate status removed. In response to earlier complaints, TRUSTe had made a public pledge to remove all false claims of non-profit status within 12 months.[12] That pledge was made in 2009, but by 2013 hundreds of TRUSTe certified companies were still claiming that TRUSTe was non-profit, and it was clear that a formal complaint to the FTC was necessary. It was always very difficult to understand how these false claims survived when TRUSTe claimed to conduct annual re-certifications.

---

[10] Chris Babel, CEO 'TRUSTe's Agreement with the FTC' (TRUSTe blog, undated) <http://www.truste.com/blog/2014/11/17/truste-ftc/>

[11] The proposed consent order prohibits TRUSTe from making any further false or misleading claims regarding "the corporate status of Respondent [TRUSTe] and its independence" (emphasis added). TRUSTe, was originally a non-profit organisation from 1997-2008, and its documentation described it as 'an independent, non-profit organisation'. It had been a for-profit corporation since 2008, but it had 'recertified clients who had failed to upgrade references to the company's for-profit status'. This was considered by the FTC to be a deceptive practice. The prohibition in the consent order also applies to misrepresentation made via organisations certified by TRUSTe. 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.

[12] TRUSTe, *Trustmarks: A Decade Advancing Privacy for Businesses and Consumers*, 2009 White Paper, p.19

APEC CBPRs' misplaced trust in TRUSTe

The APEC Cross Border Privacy Rules system (APEC CBPRs) has been operating for 18 months. The in-principle deficiencies of the system, and the deficiencies of how it decides that countries are fit to participate, are well-documented.[13] Over 100 individual company websites now claim to be APEC-CBPRs-compliant in their privacy policies, and the number is growing rapidly. The potential for large-scale consumer reliance on these policies is therefore increasing rapidly. TRUSTe is the only Accountability Agent (AA) for the United States, and the only AA appointed anywhere under CBPRs as yet. This first implementation of the APEC CBPRs has failed to meet even the most basic of APEC's own Privacy Framework requirements.

Summary of deficiencies of APEC CBPRs operation with TRUSTe as AA

The following deficiencies are detailed in the rest of this section.

1. *Recognition criteria* The APEC recognition criteria for AAs have been comprehensively ignored – TRUSTe's program requirements are a weak subset of APEC's own criteria;

2. *Conflicts of interest* TRUSTe has been certifying companies that share the same owners and directors as TRUSTe, in apparent breach of the APEC Conflict of Interest requirements;

3. *Impermissible exclusions* Companies have been including very extensive exclusions in the fine print of their privacy policies that completely undermine the APEC requirements;

4. *Unsubstantiated certification claims* There are already numerous claims of APEC certification not supported by the TRUSTe or APEC CBPRs websites, even after less than 18 months of operation, and without any sign of this apparent deception being detected or investigated;

5. *Conflicting certification lists* There is no authoritative up-to-date list of certified companies, on either the TRUSTe or CBPRs websites, which are in conflict; and

6. *No renewal dates* 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.

Civil Society organisations have already brought all of these matters to the attention of the administrator of the APEC CBPRs (the Joint Oversight Panel or JOP), some as far back as March 2013 and it has failed to act upon them. TRUSTe's required 'annual' renewal of its AA status is now nearly half a year overdue, during which time it continues to mislead

[13] Greenleaf, G 'APEC's Cross-Border Privacy Rules System: A House of Cards?' (2014) 128 *Privacy Laws & Business International Report,* 27-30; Greenleaf, G 'APEC's CBPRs: Two years on – take-up and credibility issues' (2014) 129 *Privacy Laws & Business International Report,* 12-15.

consumers, with the JOP's knowledge and implied approval.

Non-compliance with APEC recognition criteria for AAs

The APEC recognition criteria for Accountability Agents (AAs)[14] have been consistently ignored both by the JOP and by the only AA appointed to date (TRUSTe) – TRUSTe's program requirements are a weak and non-compliant subset of the APEC criteria. After civil society intervention, TRUSTe was forced to develop and publish specific APEC CBPR program requirements.[15] However, these revised TRUSTe program requirements do not meet key AA Recognition Criteria, as the JOP was informed but persisted with recommending certification nevertheless.

Examples of failures include: There is no "notice of collection" requirement for any circumstances other than online collection of data (Criterion 2); There is no requirement for collection to be *fair* (Criterion 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 (Criterion 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. (Criterion 30); The requirement that access to personal information must be provided within a reasonable time is missing (Criterion 37B); The requirement that correction should be provided within a reasonable time is missing (Criterion 38C); and the restriction on third parties undertaking further sub-contracting without consent is missing (Criterion 47).

It should be 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, 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 (including TRUSTe) in order to regain credibility.

Conflicts of Interest

For 18 months, TRUSTe has been certifying companies that share the same owners and directors as TRUSTe, in clear breach of the APEC CBPRs Conflict of Interest requirements. The Australian Privacy Foundation warned the JOP in 2013 that conflicts of interest would be a major issue for TRUSTe, and submitted TRUSTe should not be recognised as an AA without investigating whether it 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

[14] APEC recognition criteria for AAs: <https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Application%20for%20APEC%20Recognition.pdf>.

[15] TRUSTe APEC CBPR program requirements: <http://www.truste.com/privacy-program-requirements/apec>

CBPR system, two of them already have a very significant business affiliation with TRUSTe. TRUSTe shares the same major owners with two companies it has certified, and even shares a common Director with one of them. 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 appears that TRUSTe is not in compliance with these very clear requirements.

The recent FTC enforcement action against TRUSTe 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 Privacy Policy of one TRUSTe-certified company 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 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 from Privacy Policies of other TRUSTe-certified companies. One states: "The TRUSTe program does not cover information that may be collected through downloadable software, SaaS offerings, or mobile applications." Another states: "This policy does **not** apply to personal information collected from offline resources and communications."

These are all breaches of the APEC CBPRs which requires comprehensive coverage of all personal information collected from any source.[16] They will result in consumers being misled by all of these companies because consumers will understandably assume, based on the

[16] 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>.

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.

Unsubstantiated 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 apparently deceptive and potentially fraudulent conduct being detected or investigated. 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. A number of sites that claim to be APEC CBPRs compliant, but are not listed, have been reported to APEC and to the FTC. There are more, and the number of such unsubstantiated claims is growing rapidly.

There are no resources or infrastructure in place in the APEC CBPRs system, by JOP or by the FTC as the USA's APEC CBPRs enforcement agency, to detect this type of apparent 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 of Safe Harbor membership 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 companies making false claims, and announce publicly that they are doing so.

Incomplete and conflicting lists of certified companies

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.

After 18 months of operation, and numerous requests, there is still no authoritative list of certified companies available. A temporary list on the CBPRs website was finally provided in late 2014, but 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. It is constantly out of date and it is not 'synced' to the list of APEC privacy seals maintained by TRUSTe. The list 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 that have issued major press releases announcing their TRUSTe APEC certification – even when these press releases are issued by TRUSTe itself. Again, the list does not provide any contact information – it is just a column of company logos.

Both lists will mislead consumers as they are both incomplete, and the inconsistency adds to the confusion. APEC 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 not being administered as it is required to be, placing customer privacy at risk.

No expiry dates known

Both TRUSTe and APEC have 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 have begun 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.

APEC's JOP is fully aware, as a result of submissions made by the Australian Privacy Foundation, that key information on renewal and expiry dates has been withheld from consumers. The FTC's COPPA/Safe Harbor case against TRUSTe 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.

Process issues in certification and re-certification

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 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 meaningful way and, by extension, to the many problems highlighted above. In the meantime, the CPBRs continues to operate as though there were no serious question marks over its integrity.

Civil Society petition to APEC and FTC

Civil Society organisations have called 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, if it is to continue.

As documented in this article, Civil Society organisations state that current CBPRs

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 apparent false claims of APEC certification, without any detection or enforcement action.

Civil Society organisations have therefore called upon APEC to do the following:

(i) to refuse to renew the AA status of TRUSTe.

(ii) 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.

(iii) to open up key aspects of the APEC CBPRs, including the AA certification and renewal of certification processes to proper consultation with stakeholders, including civil society representatives.

(iv) 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 conclude that the current implementation of the APEC CBPRs is doing more harm than good and needs very urgent and extensive reform if it is to continue.

Conclusion: Self-regulation in crisis?

As the first AA in APEC CBPRs, and a participant in COPPA and the EU-US Safe Harbor, TRUSTe is a key part of the self-regulation approach to privacy. In each case the self-regulation scheme is endorsed by governments, and in each case TRUSTe has been exposed as a weak link. Regulators and government participants in these self-regulatory schemes have been slow to respond to warnings about TRUSTe, and have allowed the schemes to be undermined by deceptive conduct, conflicts of interest, false claims of certification, fine print exclusions and general non-compliance with the core requirements of each scheme.

The recent FTC enforcement action against TRUSTe is a wake-up call for the sector, but much more needs to be done before integrity is restored.