Application by TRUSTe for recognition as an Accountability Agent under the APEC Cross Border Privacy Rules System:

Civil Society comments on the Joint Oversight Panel 'Addendum', April 2013

Comments by Nigel Waters, in consultation with other Civil Society colleagues.

These comments are endorsed by the Australian Privacy Foundation http://www.privacy.org.au and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) http://www.cippic.ca/en

8 May 2013

Contents

Executive Summary

Civil Society stakeholders provided brief comments on the original JOP recommendation to approve TRUSTe's application as an AA. The JOP have responded with some further information in the Addendum. This document sets out our further comments on the JOP Addendum. Our comments and suggestions are put forward as constructive criticisms to assist APEC economies to fashion a CBPR process with high integrity, credibility and transparency.

In summary, we find that

- TRUSTe has not shown that it complies with the key Program Requirements that were questioned – with very few exceptions neither JOP nor TRUSTe has provided any new information that demonstrates compliance. TRUSTe's application does not demonstrate compliance with at least 21 of the Program Requirements.
- In many cases, the supposed compliance with a Program Requirement is not documented, but it is simply asserted that 'the JOP has confirmed that' TRUSTe complies with the requirement, often without a detailed explanation of how it complies. This is completely unsatisfactory as APEC member economies should be able to assess each AA criteria against documentary evidence of compliance.
- In any case where compliance is not documented in an AA's Program documentation, this should not be acceptable, because (a) it is not in a form which is transparent to data subjects, DPAs or others; and (b) in the case of the USA, it will not constitute the type of written holding-out to the public that can result in a breach of s5 of the FTC Act.
- Statements by the JOP, whether public or not, cannot meet the above requirements, they must be public statements made by the Accountability Agent itself;
- The JOP Addendum has failed to resolve key issues regarding the applicability of TRUSTe's processes to offline activity, jurisdiction, conflicts of interest and reporting requirements.

Any of these deficiencies should be, in our view, sufficient to result in a decision that TRUSTe's application has not met the APEC CBPR requirements. We submit that APEC member Economies should determine that TRUSTe has not met the requirements to participate as an Accountability Agent, having failed to meet (in an appropriately documented fashion) all the Program Requirements, and that strict adherence to full compliance should be required in light of the overall deficiencies of the application in demonstrating the desired transparency and substantive integrity of the CBPR process. It is appropriate for such a decision to be made at this stage of the process.

In many cases the JOP has not dealt with the substance of the inadequacy of TRUSTe's approach, and the effect that its deficiencies might have on the overall credibility of the CBPR system – particularly since this is the first assessment of an Accountability Agent – but have instead resorted to repetitively stating that 'Should Member Economies wish to require that [insert issue here] they may expressly incorporate such requirement into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).' This is done on eight occasions. This approach gives preference to technicalities at the expense of focusing on the long-term needs of the credibility of the CBPR system. Interestingly, no such limitations were raised in the initial JOP recommendation – it simply stated that TRUSTe was compliant against each and every criteria.

Submission

Our submission is divided into two main sections – an analysis of TRUSTe's compliance with the AA criteria, based on the numbered table marked as Annex A in the Addendum, followed by a general discussion of non-compliance with other AA criteria. Some concluding comments are made on the accreditation process, and the need to ensure that initial applications are of the highest standards.

Program Requirements

Table mapping against AA Criteria – TRUSTe fails to meet 21 criteria

The TRUSTe program requirements cannot be successfully mapped against all AA Criteria, based on the information provided to date. On our analysis, taking into account the JOP comments, TRUSTe's application still fails to comply with 21 of the 22 Program Requirements set out in the Table following.

A key starting question for this analysis is: Which TRUSTe program requirements is the JOP actually assessing? There are numerous existing TRUSTe programs, each with different requirements (e.g. website, email, software download, mobile apps, children, EU Safe Harbor etc.). There are no published APEC privacy seal requirements at this stage.

The JOP analysis appears to quote from the core TRUSTe privacy program, with occasional strange references to the EU Safe Harbor seal requirements. However, that core program only applies to online activities, and even then it excludes software downloads, mobile apps etc. The Addendum states that APEC will develop a new APEC seal, but claims that the existing program requirements will apply. Obviously we don't believe that this approach is correct, but for the purposes of simplifying the discussion, we will persist with the approach set out in the Addendum, and attempt to match the AA criteria against the core TRUSTe requirements.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
2	Notice of collection	TRUSTe only requires a privacy policy to be available. There is no notice requirement for any other circumstances (e.g. application forms, collection over phone etc.)	TRUSTe's program requirements state that the privacy policy must be present when information is collected. (III.D.5)	This is completely wrong. That section is in relation to online privacy statements, and is requiring the company to EITHER link to the policy on the page where information is collected OR place the link in a common footer on every page. There is absolutely no reference in that entire section to any offline activity. The JOP interpretation is a complete reinvention of the section, and is the opposite of TRUSTe practice for more than a decade. TRUSTe privacy policies specifically exclude any information that is not collected via the website (e.g. by software download). Why would TRUSTe require organisations to give offline consumers a copy of a privacy policy that specifically excludes offline activity? The JOP should point to specific TRUSTe documentation for the APEC seal that provides evidence of compliance with this requirement.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
3	Notice of 3rd party use	Not a TRUSTe program requirement	TRUSTe's notice requirements around use cover both first and third parties and do not distinguish between first and third parties. Further third-party disclosure is still required.	TRUSTe's other requirements include extensive discussion of Third Parties, so their complete absence from the use section would likely be interpreted as deliberate. If this is not the case, then the TRUSTe APEC seal documentation should clarify this.
7	Lawful and fair collection	TRUSTe only requires activities to be lawful and not misleading. There is no test of fairness.	Section 5 of the FTC Act, 15 U.S.C. § 45 gives the Federal Trade Commission (FTC) broad authority to take action against unfair and deceptive acts and practices. As noted in TRUSTE's Master Services Agreement "Participant represents that it understands that it has an independent duty to comply with any and all laws and regulations." As such, fairness is a component of lawfulness in this instance.	This is an unjustifiably broad and generous interpretation of the TRUSTe requirements. Are TRUSTe now certifying compliance with every other law in the US because the client has stated that it 'understands' it has other independent duties to comply with the law? If fair collection is an APEC requirement then an AA approved by APEC should take some responsibility for ensuring compliance with fair collection. The result of the JOP approach is that if a back-stop law exists, as it does in this case in relation to the broad concept of fairness, then there is no need for the AA to have any criteria itself. Surely it would be easier to just add 'fair collection' to the TRUSTe APEC seal requirements. It is a key component of the privacy requirements in every other APEC jurisdiction with laws in place. APEC has spent years developing a framework, principles, CBPR rules and AA criteria that all require 'fair collection'. Why would this test suddenly be abandoned for TRUSTe?
8	Use limited to the purpose stated at the time of collection	The TRUSTe program requirement says that use is limited to any purpose 'reasonably useful' for the purpose stated at the time of collection. It is unclear what this test means in practice, but it is obviously different from the APEC core principle and should be subject to further analysis.	TRUSTe's Program Requirement III.C.2a limits use of personal information to " the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements." Program requirement III. C.1 further limits collection "to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection."	The JOP response does not answer the question, it simply repeats the information previously provided by TRUSTe. Surely there is a significant difference between "use limited to the purpose stated at the time of collection" (APEC) and "any purpose reasonably useful for the purpose stated". Why is the TRUSTe requirement so much looser than the APEC requirement?

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
22	Correction of inaccurate data	TRUSTe limits this requirement to 'commercially reasonable steps'. There is no discussion or analysis of this limitation.	Reasonableness as a standard is found throughout the CBPR Program Requirements. Access and correction includes three qualifications, including "disproportionate burden." This qualification states that "[p]ersonal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature." Given the program requirements themselves provide no further analysis of reasonability, the JOP has no endorsed basis upon which to assess TRUSTe's references to "reasonableness" as it relates to the program requirements under integrity (see TRUSTE program requirements III.E.3.a and III.C.5.a, b).	"Commercially reasonable steps" is clearly a much lower test than "unreasonable or disproportionate to the risk". Again, why can't TRUSTe adopt the same tests that appear in the APEC requirements? Why has the JOP found a lower test to be compliant with this important APEC requirement? If APEC wanted to adopt a lower test – commercial reasonableness – they would have chosen those words. They did not – they specifically chose the term "unreasonable or disproportionate to the risks". This is such an obvious difference that it is difficult to understand the JOP's refusal to re-open discussion of TRUSTe's compliance with this criteria. At the very least the core APEC balance between the cost, on one hand, and the **risk**, on the other, should be re-established. TRUSTe does not even include risk in the equation.
23 and 24	Correction of inaccurate data to be forwarded to agents and relevant 3rd parties	Not a TRUSTe program requirement	The obligation of the participant also obligates the service provider in section III.E.5.a.1 – 2. As such, the participant's obligation to maintain accurate data includes an obligation to ensure third parties, specifically service providers, have accurate data in the first instance.	The JOP response completely misses the point of this section. The APEC requirement requires forwarding of corrections AFTER they are discovered, at any time. The TRUSTe requirement is limited to accuracy "in the first instance" – to quote the JOP's own words. The distinction is clear – TRUSTe is clearly not compliant.
25	Agents and 3rd parties to inform organisation regarding inaccurate data	Not a TRUSTe program requirement	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.	There is no Section III.E.A in the TRUSTe program. It does not exist in the public version of the TRUSTe program requirements. There do not appear to be any requirements that meet this specific APEC test.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
29	Staff to be informed and trained re security policy	Not a TRUSTe program requirement	The JOP has confirmed that TRUSTe interprets "reasonable security measures" to include the requirement of staff engagement and training.	The JOP may have received verbal assurance of this interpretation, but how does that help TRUSTe meet the APEC requirements for AAs? In the US these requirements will only have legal force (via s5 FTC Act) if they are available in public documentation. Also, did the JOP receive this confirmation in their initial decision, or only after concerns were raised? Where is training even mentioned in any TRUSTe document?
30	Safeguards have to be proportional to (1) sensitivity of information; and (2) the probability and severity of the harm	The TRUSTe test is proportional to 'size of the business' and 'sensitivity of the data'. This appears to be a completely different test.	The JOP has confirmed with TRUSTe that a determination of the sensitivity of the information incorporates consideration of the severity of the harm.	The JOP may have received verbal assurance of this interpretation, but how does that help TRUSTe meet the APEC requirements for AAs? In the US these requirements will only have legal force if they are available in public documentation. Also, did the JOP receive this confirmation in their initial decision, or only after concerns were raised? The reference to 'size of the business' has absolutely NO bearing on the APEC requirement. 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.
35B, 47)	(Following transfer) 3rd parties must be required to promptly notify the organisation of a breach	Not a TRUSTe program requirement	TRUSTe requires the participant to provide data breach notification and to impose equivalent obligations on its third party service providers. As such, third-party service providers must provide notice to the participant for any data breach.	Where is this stated in the TRUSTe program requirements? The JOP / TRUSTe have not referenced any section numbers here. There is a broad security section (already severely limited by the inappropriate 'size of the business' test discussed above), and a very general requirement to ensure that service providers are complying with the participant's *published privacy policy* (our emphasis), but there are no other relevant requirements. The participant's privacy policy is unlikely to include any reference to data breach notification requirements – unless there is a massive change in TRUSTe practices. This is actually a very simple and specific requirement that should be added to the TRUSTe program in order to comply with the AA criteria.
37A	Steps to verify identity of persons seeking access	Not a TRUSTe program requirement	TRUSTe access program requirements are related to an "individual." The JOP has confirmed that TRUSTe defines this as the actual data subject. Disclosure of personal information to anyone beyond the data subject would violate TRUSTe's program requirements for both first party and third-party disclosures. Thus, ID verification is required when allowing the "individual" access and correction rights.	The actual question in the AA criteria is: 37. a) Do you take steps to confirm the identity of the individual requesting access? It is difficult to think of a more straightforward question than that. The JOP and/or TRUSTe must answer this question – yes or no – and provide evidence that this is included in the TRUSTe program as a specific requirement. It does not appear to be mentioned anywhere in the TRUSTe program and JOP/TRUSTe have not referenced any section numbers here.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
37B	Access to be provided within a reasonable time	TRUSTe allows initial period (30 days) to be extended indefinitely. No test of 'reasonable time'.	TRUSTe program requirements IV.A.1.a-b require that the provision of access beyond the default 30day period be limited to the timeline established in the participant's privacy statement. The program requirements provide no explicit basis upon which to assess "reasonableness" as it relates to this program requirement. Absent specific guidance, the JOP has determined in its opinion that a default 30 day timeline limited to pre-defined exceptions (to be assessed in advance by TRUSTe) meets this standard.	The JOP response assumes that the default period is 30 days. This is a serious error. In fact, the main TRUSTe program does not include *any* timeline or any requirement for a timely response. Those requirements ONLY appear in the additional requirements for EU Safe Harbor certification, as they are an EU regulatory requirement. They only apply to a small fraction of TRUSTe clients, and far from being the 'default' setting, they are actually the exception. The JOP /TRUSTe should have, but have not provided documentary evidence that the timeliness requirements will be included in the APEC seal program. (NOTE: The 30 day error is included in several responses in the initial JOP report – we haven't looked for and corrected all of them in this response)
38C	Correction to be provided within a reasonable time	Not a TRUSTe program requirement	US law presumes a "commercially reasonablity" standard on all activities which do not have otherwise specified timeframe's associated with them. Since the TRUSTe program requirements offer a right of correction, they must be within a reasonable time under US law.	APEC member economies have spent the best part of a decade negotiating the privacy principles, the CBPR regime and the AA criteria, and they have chosen to include a specific requirement that corrections must be provided within a reasonable timeframe. This is a simple, straightforward requirement. The JOP / TRUSTe should provide documentary evidence that this criteria has been met. How will TRUSTe clients even know that this APEC requirement exists if it is not included in the program? There may well be a back-stop legal requirement related to reasonable timeframes, but the whole point of the TRUSTe program is to promote up-front good practice, and to allow consumers to have matters resolved without having to engage in expensive litigation. The concept of 'commercially reasonable time' has been the subject of extensive and confusing litigation in the US, with every single case being decided on its individual elements and circumstances in very expensive court cases. Is this really a solution for TRUSTe customers?
38E	Rights following refusal of correction	Not a TRUSTe program requirement	TRUSTe program requirement III.C.5(h) states that "If Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access."	We concede this is correct and that our initial comment was wrong.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
39	Measures to ensure compliance	TRUSTe program limits this section to measures 'Appropriate to the size of the Participant's business' – this cannot be right (possibly a mistake in completing the form).	In the opinion of the JOP, TRUSTe program requirement III.E.1.a.1 ("Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E") meets the requirement that a participant ensures compliance with its privacy program requirements.	The JOP has not responded to the specific concern raised in relation to criteria 39. Limiting compliance to measures 'appropriate to the size of the business' is not part of the APEC Privacy Framework. APEC does have a 'harm' test, but that is completely unrelated to the size of the business. Many small companies have caused significant privacy harm, and even in the US the FTC has taken action against small firms for false claims made in their privacy statements. The 'size of the business' test should be removed.
40	Appointment of an individual with overall privacy compliance responsibility	Not a TRUSTe program requirement (although the master agreement does require the maintenance of a central email contact point)	The JOP has confirmed that TRUSTe's *Master License and Service Agreement Program Amendment – Privacy Program* requires the granting of authority by the participant to a named individual to manage the obligations of the privacy certification. In addition, the *Master Services Agreement* section 11(f)) creates a Designated Participant Coordinator responsible for all matters related to any TRUSTe certification, including but not limited to the unique CBPR web seal to be administered by TRUSTe.	It is not clear that this is a fair response to the AA criteria. It was not included in the original JOP report and there has been no prior mention of the various Amendment Agreements to the Master Services Agreement. Are these all available as public documents? Which of the many documents is the JOP referencing here? Can stakeholders review copies of the amendment agreements? Does one exist that is relevant to APEC CBPR? (The quoted document appears to only apply to online activity).
42	Initial complaints process to be 'timely'	Not a TRUSTe program requirement for its participants	The applicable TRUSTe requirement (III.E.6.a) mandates such procedures be "reasonable, appropriate, simple and effective." The JOP is satisfied that this standard encompasses timeliness.	The JOP may be 'satisfied' that timeliness is included, but this should be reflected in the documentation. Again, APEC has worked for many years to include a requirement that complaints will be dealt with in a timely manner, why should this not be included in the TRUSTe program? How does this differ from any other AA criteria? If it is not a written commitment how can it be enforced by the FTC if required?
43	Explanation of remedial action	Not a TRUSTe program requirement	The JOP has confirmed with TRUSTe that Program Requirement III.E.6.a includes an explanation of any subsequent remedial action taken.	That is an unjustifiablly generous interpretation of 6a, which states (in full): 'Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.' There is absolutely no mention of the provision of an explanation of remedial action. The JOP/TRUSTe should provide written documentation showing compliance with this criteria – a verbal assurance is not sufficient.

Q	Issue	Civil Society original query	JOP Addendum response	Civil Society further comments
44	Staff training for compliance and complaints	Not a TRUSTe program requirement	The JOP has confirmed that TRUSTe interprets "reasonable security measures" under III.E.2a-b.1-4 to include the requirement of staff engagement and training.	There is no mention of training in the sections referenced by the JOP. There is, however, quite a specific list of security measures, including encryption etc. The absence of training from such a specific list implies that it is not a requirement. But the main issue here is that criteria 44 requires training in relation to compliance and complaints – the JOP has only referenced sections dealing with security. Are these sections even relevant to training related to complaints? All stakeholders should read criteria 44 – it is very specific. Where is the documented evidence that TRUSTe has ever considered staff training regarding complaints as a program requirement?
47	Restrictions on 3rd parties undertaking further sub-contracting without consent	Not a TRUSTe program requirement	The JOP has confirmed that TRUSTe requires that the obligations a participant imposes on third parties apply to any sub-subcontractors in the same manner under II.E.5.a.1-2.	The section referenced by the JOP has no bearing at all on the issue raised in Criteria 47. If the JOP has somehow 'confirmed' that the TRUSTe program requires 3rd parties to seek consent before undertaking further sub-contracting work, that is likely to be news to TRUSTe participants. The JOP / TRUSTe should provide documentary evidence that this criteria applies in the TRUSTe program.
48	Verification of self assessments	Not a TRUSTe program requirement	The JOP has confirmed that III.E.5.a.1-2 requires any participant to take commercially reasonable steps to ensure personal information processors, agents, contractors or other service providers comply with the participants instructions and/or agreements/contracts. As drafted, self- assessments are not a requirement under the CBPR system for such third-parties. However, when used by a participant, the Accountability Agent must verify their existence. Should Member Economies determine that such third-party self-assessments should be made mandatory for CBPR certification, it should be expressly incorporated into the CBPR Program Requirements pursuant to the established endorsement process (the consensus determination of Member Economies).	The JOP has now found that TRUSTe does not comply with this requirement, but correctly points out that it is not mandatory to impose a self assessment process on participants. This was not mentioned in the initial JOP report, which concluded that TRUSTe was compliant, and even quoted Section III.E.5 as evidence.

General comments on the Table

As can be seen from the above table, there are significant gaps in TRUSTe's compliance with the core AA recognition criteria. A major deficiency that runs through the whole of TRUSTe's

application, and the JOP's analysis, is that TRUSTe's asserted compliance with particular CBPR Program Requirements does not stem from any clear public documentation of that alleged compliance, even though such documentation is necessary in order to engage the FTC's jurisdiction. Instead the JOP merely states that 'the JOP has confirmed' compliance with some requirement or other, but without stating that this compliance is promised in some specific TRUSTe documentation. In some cases the JOP simply says 'TRUSTe requires' but does not identify any documentation of this.

In other cases it appears that the JOP is merely expressing an interpretation of what TRUSTe's policies require (and a contentious interpretation at that) – and it is unclear whether this is TRUSTe's interpretation or the JOP's interpretation.

A particularly alarming example is the claim in the JOP Addendum that Section III.D.5 of the TRUSTe program requirements applies to offline activity, therefore providing compliance with AA Recognition Criterion 2. This is completely and totally incorrect, and is the subject of detailed discussion in the table above. But is this a claim being made by the JOP or by TRUSTe? If it is being made by TRUSTe in writing, it triggers FTC jurisdiction, and that could have serious consequences. But what if it is merely an interpretation by the JOP?

This is a significant failing in the JOP process. The AA recognition criteria require an applicant to say yes or no to each criterion – but there is no document where TRUSTe has done this. If the answer is YES then documentary evidence should be provided. If the answer is NO then the AA criteria sets out a different process for establishing compliance for each criteria, which if not satisfied should presumably lead to the application being rejected. There is no evidence of an alternative basis for satisfying the criteria.

Again, looking at the claim regarding Section III.D.5 above, if this claim has been made by TRUSTe then it completely rewrites 16 years of TRUSTe history. It means that nearly 5,000 TRUSTe certified companies are suddenly covered by the TRUSTe privacy requirements for ALL of their activities, even though the typical TRUSTe privacy policy states clearly that it only covers information collected by the website. Does it mean that all of TRUSTe's other programs are irrelevant (email, downloads, mobile apps, smart grid) because Section III.D.5 already magically covers all of those activities? Why have companies been paying TRUSTe for additional services if the interpretation of Section III.D.5 is correct? Can we re-open all of the famous complaint cases that TRUSTe rejected because they didn't relate to the specific website covered by the seal program? (e.g. Microsoft UID, RealJukebox and other similar cases).

Obviously, none of this is going to happen. Section III.D.5 only applies to online activity, and even then it is restricted to the specific website covered by the privacy seal. TRUSTe are very unlikely to have claimed otherwise, and they are unlikely to stand by the claim now.

So is it a claim by the JOP? If it is wrong (which it is), then it should be replaced with a finding of non-compliance in relation to AA Recognition Criterion 2. Alternatively, TRUSTe could resubmit a new and amended application at some future date and provide documentary evidence of compliance with the criteria. This would require them to design a new seal program that includes coverage of offline activity.

The claim that Section III.D.5 of the TRUSTe program requirements applies to offline activity is therefore a ridiculous and unsupportable claim, which APEC economies should summarily reject.

We also note that the JOP Addendum only provides commentary on a small selection of criteria – these were the ones highlighted by Civil Society stakeholders. We noted in that letter that we had *not* conducted a comprehensive analysis and the list was not exhaustive. For example, we were unable to undertake a detailed analysis of AA recognition criteria 8-12 and criterion 39 and criterion

49, as information on TRUSTe's approach in these areas is extremely limited. Yet the JOP have only chosen to re-examine issues that were specifically raised in the letter. It is likely that there may be more gaps, as the JOP's consideration of the TRUSTe program has been very minimal.

Other AA requirements

Applicability: No offline data privacy practices can be covered at present

The JOP has failed to make any detailed response to this issue, and it is possible that the JOP members have failed to grasp the seriousness of this gap in TRUSTe's application.

TRUSTe currently runs a large suite of certification programs. All of them apply only to online or mobile activities. The detailed program requirements and the master services agreement make numerous references to 'online property'. TRUSTe's terms and conditions restrict their own access (e.g. for investigations) to a client's online resources.

TRUSTe also has numerous investigative and monitoring tools available, but all of these relate to online or mobile activities, such as seeding email lists or monitoring websites. They have no tools or processes for monitoring offline activity. They have not pointed to any experience in relation to offline activity.

If TRUSTe are to extend their certification to offline activity, for what appears to be the first and only time in their history, the JOP should be making detailed inquiries as to how this will be done. When and if TRUSTe submits a new application, it should be required to provide a documented plan as to how they will deliver this new service within their existing business model, fee structure and resources.

Importantly, TRUSTe should have provided detailed program requirements and terms and conditions relating to offline activity for consideration by APEC, but did not do so.

They should also have provided samples of the wording that they propose to use for consumers, but did not do so. At the moment, when you click on a TRUSTe seal it will state: "The privacy practices of this site have been certified by TRUSTe for compliance with the following programs: [name of program]." And if you follow the links you will be provided with information about how TRUSTe works in relation to websites. There is no information about offline activities at all, and TRUSTe holds itself out only to have examined online activities.

Indeed, the standard wording of a privacy policy certified by TRUSTe includes the following words (or similar):

> The TRUSTe program does not cover information that may be collected through downloadable software. The TRUSTe program covers *only* information that is collected through this Web site, www.example.com

A completely new approach (and a new application) should be required if TRUSTe is going to act as an AA for APEC, where there is no distinction between online and offline activities. The JOP and APEC members should be given a proper opportunity to consider this new approach.

It is completely baffling that the initial JOP recommendation made no mention at all of offline activities, despite this being a clear APEC requirement. The subsequent attempt to claim that offline activities are covered by Section III.D.5, is equally baffling.

It is very important, indeed essential, that any favourable JOP recommendation or APEC decision would have to restrict the approval of TRUSTe as an AA to cover only online activities of organisations. Of course, we do not consider that there should be any such favourable decision.

Jurisdiction: A quarter of the US market is excluded

The initial JOP report and the Addendum both dismiss concerns about jurisdiction, however it is important to note that if a US company is not within the FTC's jurisdiction, then they cannot be covered by the APEC CBPR Framework, as there are no other APEC recognised privacy regulators in the US.

The JOP Addendum states: "It does not appear that TRUSTe engages in any activities that would preclude or limit FTC jurisdiction". That may be the case, but what about the entities who are certified by TRUSTe? How can TRUSTe refer a member to the FTC (in the enforcement context) if the FTC has no jurisdiction? How can s5 of the FTC Act supply some of the substantive compliance with Program Requirements (as JOP claims) if the FTC has no jurisdiction?

This is not a trivial or a technical matter, but goes to the essence of this accreditation. The FTC has no relevant jurisdiction over banks, insurers, airlines, some telecommunications carriers and a large number of other businesses, many of which are currently certified by TRUSTe. The JOP appears willing to simply dismiss the jurisdiction question, but we are actually talking about excluding 20-25% of the US market.

There are also numerous situations where the FTC does have some limited jurisdiction over one aspect of a US company's business, but has no jurisdiction over the rest of the business. For example, where a telecommunications company is engaged in common carrier activity, the FTC has no jurisdiction. But when the same company is engaged in billing its customers or facilitating mobile payments, the FTC does have jurisdiction. There are many other examples.

It is very important, indeed essential, that any favourable JOP recommendation or APEC decision should restrict the approval of TRUSTe as an AA to cover only those organisations that are subject to FTC's relevant jurisdiction, and only those activities that are within FTC's jurisdiction. Of course, we do not consider that there should be any such favourable decision.

Conflicts of Interest: TRUSTe is not independent of those it regulates

In relation to the important issue of conflict of interest, the JOP avoids the substantive issues in its Addendum response. We adhere to the view that the conflict of interest issue is so important that TRUSTe (and any other AA applicant in future) should be required to provide to the JOP and make public a formal written Conflicts of Interest policy signed off by their Board.

The JOP has not responded to our earlier request to ask TRUSTe whether any TRUSTe directors or owners are also directors and/or owners of sites certified by TRUSTe. This is an important issue.

TRUSTe is in a unique and unacceptable situation for an AA, in that no other privacy accountability agent is asked to manage complaints and potential enforcement action against companies which share the same owners or directors. There are certainly no other examples of privacy regulators who are directors of the companies that they regulate. In this context it is essential that TRUSTe publish a conflicts of interest policy, endorsed by the Board, that explains how TRUSTe deals with these types of conflicts. When a consumer clicks on the TRUSTe seal on a website, they are told that TRUSTe is "an independent third party". This statement appears on every site, whether or not there are any corporate links between TRUSTe and the client. APEC must ensure that this claim is accurate and that TRUSTe has conflicts policies and procedures that will stand up to scrutiny.

The actual test in the AA Recognition Criteria states:

> "At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the CBPR System…" (Accountability Agent Recognition Criterion 2(a) and (b))

Each APEC Member Country should be making detailed inquiries about how TRUSTe can meet this criteria. We suggest that it is unreasonable and unfair to the members of the JOP to expect them to have to attest to the adequacy of a secrety conflicts policy, apparently without any further investigation.

We urge each APEC Member Country to question whether it can support a system where:

1. TRUSTe is approved by APEC as the AA for the US;
2. TRUSTe is a for-profit corporation that earns all of its income from fees collected from the organisations it certifies;
3. TRUSTe shares owners and directors with some of the companies that it certifies;
4. TRUSTe tells consumers who click those companies' seals that TRUSTe is "an independent third party", with no further disclosure; and
5. TRUSTe has no public conflicts of interest policy, and only the 3 member JOP has examined the confidential policy.

The JOP Addendum attempts to allay concerns about conflicts by pointing out that Directors of TRUSTe are bound by US law to be loyal to TRUSTe. Where those same directors are also directors of client companies, they are equally bound by law to be loyal to those companies. This assurance is not useful in the special circumstances that apply at TRUSTe. They have no obligation to be loyal to the data subjects whose interests they are supposed to protect in order to fulfil APEC's CBPR mission. They clearly have conflicting loyalties and conflicting interests, as does TRUSTe in consequence.

Certification process: No one knows what full TRUSTe certification costs

The JOP has explained that they have reviewed the *existing* certification process, including looking at the current forms in use by TRUSTe. They have concluded that the certification process is adequate, and they have noted that there is no requirement for them to consider other issues such as business models and fees.

We submit, again, that it is essential for APEC Member economies to have some confidence in the adequacy and viability of the certification process. Studying the existing arrangement may not be helpful in this regard. The existing program ONLY applies to online activities, and these activities are much easier to check (using online tools) than offline activities. For example, the main TRUSTe certification process does not need to examine any software, downloads, apps, telephone call centre operations, offline forms, retail outlets etc., because all of these activities are specifically excluded from the TRUSTe program (unless you purchase other TRUSTe products, such as the download seal).

The core certification program, which has been examined by the JOP, is a quick and simple certification of a website privacy policy. TRUSTe has previously offered a starter pack seal for under $500 USD (this pricing may have changed). This probably reflects the ease with which a website privacy policy can be assessed. However, they have additional programs (at additional cost)

for examining email, mobile apps, software downloads, targeted advertising, smart grids and other specific activities.

In this context, what steps has the JOP taken to assess the adequacy and viability of TRUSTe's certification processes that will be relevant in APEC CBPR? Have they examined these other TRUSTe products? Have they considered what steps TRUSTe would need to take in order to assess compliance in relation to offline activities? The JOP Addendum states that TRUSTe has now decided to offer a separate APEC seal, as a new stand-alone product. Can the JOP point to documentary evidence of the proposed certification process for that seal?

Ongoing Monitoring and Compliance Review: No comprehensive policy

AA Recognition Criterion 6 states that "Accountability Agent has c*omprehensive written procedures* designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program." All that we asked was for TRUSTe to provide documentary evidence of how it will monitor offline activity. No evidence has been provided.

TRUSTe has claimed that they may initiate an investigation following a media report or a complaint – that is not monitoring, that is merely responding to an issue that is already public knowledge. Is that the intention of the AA Criterion?

In practice, TRUSTe does engage in some ongoing monitoring, as it has developed useful tools for automatically monitoring online activity. But the APEC CBPR regime is not restricted to online activity. AA Recognition Criterion 6 specifically asks for "comprehensive written procedures". Where are they?

Recertification: No documentary evidence provided of a compliant TRUSTe process

The JOP Addendum includes new information regarding re-certification, that was not included in the original response or in the TRUSTe application.

In particular, the JOP rely on a claim by TRUSTe that they undertake a series of steps, including:

> "An assessment of compliance, which will include verification of the contents of the self-assessment forms (Project 1) updated by the Participant…"

It is very unclear what document the JOP is quoting from when they make this claim. They assert that this is evidence of TRUSTe's re-certification process, but this does not appear to be a TRUSTe document. It includes a reference to "Project 1" which we presume is a reference to previous APEC internal 'Pathfinder' projects.

The AA application process requires TRUSTe to provide documentary evidence of a viable re-certification process that meets the various APEC recognition criteria. These requirements cannot be met by re-quoting out-dated APEC documentation.

It is very important that the JOP clarify who is making claims such as this one – is this a claim by TRUSTe that they meet the criteria, based on the quoted 'evidence', or is the JOP making the claim itself?

Dispute Resolution: No value and 'no signs on the door' for consumers

The JOP Addendum avoids the substantive issues here. We adhere to our view that there is insufficient evidence that TRUSTe will be able to meet the requirement of Recognition Criterion 12 to be able to 'require the Participant to remedy the non-compliance within a specified time period' or the requirement of Recognition Criterion 13 to impose '... Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent'. In the absence of any evidence, Member economies need to consider whether they are comfortable with the first CBPR AA operating a system which appears to offer little of substance or value to consumers. Will this provide the CBPR system with any credibility?

In addition, while it is not expressly specified in the AA Recognition Criteria, there is no reference to complainants being notified of their right to complain to a PEA if dissatisfied with the outcome of TRUSTe's dispute resolution process. If a candidate AA fails to include a guarantee of such notification in its processes, we submit that this should be taken into account as a serious negative factor in its application, as a failure to sufficiently engage the PEA processes in its economy.

For consumers, this is a 'No signs on the door' policy, they have to guess which doors go anywhere because there is no assurance that the AA is going to assist them to find out.

Case Notes and Statistics: TRUSTe seeks to obscure transparency

We submit that it is unreasonable and unnecessary for the JOP to take the view that 'In consideration of the desirability (or in some instances requirement) to preserve anonymity pursuant to a dispute resolution, the JOP has recommended that Member Economies allow for case notes [and complaint statistics] to be drawn from a wider pool of certified companies …'

This argument is unsustainable because neither case notes nor statistics identify respondents. The effect of a 'wider pool' is to obscure what is really happening with the APEC CBPR system because it will be drowned in the 'wider pool'. To preserve the transparency and integrity of the CBPR system, we submit that Member economies should reject this approach.

We also cannot see how the provision of the TRUSTe Transparency Report meets the AA criteria requirements. Have member economies (or the JOP) actually reviewed a typical TRUSTe Transparency Report against the AA criteria?

The following table provides a brief overview. A more thorough analysis is required before member economies accept the Transparency Report as the sole fulfilment of the relevant AA recognition criterion (as proposed by the JOP in their initial finding):

AA Recognition Criteria	TRUSTe Transparency Report
Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number.	Number of complaints – YES Comment on significance – NO
Complaints processed during the year broken down by the outcome.	YES
When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.	NO
Comment on the significance of the complaints outcomes.	NO

AA Recognition Criteria	TRUSTe Transparency Report
Statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents and comment on the significance of the reported figures.	Some statistical breakdown provided, but no comments.

Conclusions

Retrospective application: An alarming claim

The JOP Addendum contains the following alarming claim:

> "While TRUSTe intends to offer CBPR certification under a unique seal, the JOP has confirmed that the certification and monitoring process used by TRUSTe to administer their "Trusted Privacy Seal" is the same as that provided under the CBPR seal."

This is similar to public statements made by TRUSTe. For example:

> "As TRUSTe is the first AA to go through this process [the APEC CBPR AA approval process], we anticipate it will take a couple of months to achieve endorsement and approval. Prior to the endorsement, TRUSTe can still provide certification services which can be later used to show participation in the APEC framework."
>
> From: http://www.ftc.gov/bcp/workshops/codesofconduct/

This approach assumes that the existing TRUSTe program can just be re-badged as an APEC program. This is a very alarming claim to make. The APEC CBPR seal cannot possibly just be the existing TRUSTe privacy program with a different coloured seal attached to it. The existing program does not cover offline activity, it does not include basic notice requirements, it does not include a requirement for a timely response to access requests or complaints, it does not include any monitoring of offline activity, it includes a 'size of the business' limitation, and it fails to meet at least 21 of the basic AA recognition criteria (as set out in the table above).

Surely the correct approach is for TRUSTe to develop a comprehensive, documented, APEC CBPR privacy program, with its own requirements, certification process, monitoring, and case reporting.

In addition, APEC member economies must be confident that important issues such as jurisdiction, scope of applicability, and conflicts of interest have been resolved.

The accreditation process: Finality of process and future applications

We suggest that APEC economies should now find that this application by TRUSTe does not meet the APEC CBPR requirements. This will provide an opportunity for other potential Accountability Agents for the USA to put forward applications, or for TRUSTe to consider developing its practices and documentation so that it can attempt to put forward a satisfactory application. We suggest that what should not occur is for TRUSTe to now be given a third opportunity to remedy the deficiencies in its current application, by producing documentation not previously disclosed or revealing practices not previously put forward (although we do not believe it likely that it could satisfy the criteria in the short term).

To allow TRUSTe a third opportunity to seek to demonstrate compliance with APEC CBPR standards would create a moral hazard in relation to future applications, because it would encourage applicants to only put forward limited information on compliance in order to see if they could 'get

away with it', secure in the knowledge that they could 'correct' their application if they could not. The current application shows how dangerous this could be, because the JOP does not seem to have the capacity to do the detailed investigation of an application necessary to show its shortcomings, and the JOP process only provides limited opportunity for broad consultation with experts and stakeholders. It is necessary therefore to do everything possible to ensure that initial applications are made *uberrima fides* (in utmost good faith), or risk rejection, with allowance only for minor additions or corrections., Finally, we suggest that it may be timely for APEC economies to ask some further questions about the adequacy of the accreditation process.. If APEC member economies are not satisfied that the JOP process has delivered an appropriate level of analysis of TRUSTe's compliance with the AA criteria, how could this be improved? Is it clear to member economies whether the many questionable claims contained in the JOP documentation have been made by TRUSTe, or are they claims and interpretations by the JOP (and how can such ambiguity be avoided in future)? Why did the initial JOP response not contain any of the vital information and purported 'assurances' and 'confirmations' contained in the Addendum? Why does the JOP Addendum only address issues raised in the Civil Society letter of concern, when that letter clearly stated that it was not an exhaustive list, and that more analysis should be undertaken? By addressing these matters, member economies will help ensure that the integrity, credibility and transparency of the APEC CBPR process is improved.