APEC Cross Border Privacy Rules (CBPR) system

Application from TRUSTe for recognition as a CBPR Accountability Agent (AA)

Joint Oversight Panel (JOP) Recommendation submitted to ECSG Chair 19 February 2013

Comments submitted by Nigel Waters, 11 March 2013[1]

Executive Summary

We submit that TRUSTe's application for recognition as a CBPR Accountability Agent is manifestly inadequate and in several significant respects does not meet the required Recognition Criteria.

Particularly because this is the first application, it is very disappointing and a considerable problem for the credibility of the CBPR system that the JOP has not made a sufficiently thorough assessment of the application.

We submit that it is not appropriate for APEC member economies to make a consensus determination to accept the JOP Recommendation. Further information should be sought to address the many ways in which the application does not currently meet the Recognition Criteria.

Our analysis of TRUSTe's current program standards/requirements against the CBPR program requirements indicates that it is not possible for TRUSTe to meet these requirements without major changes to its own practices.

We are particularly concerned that key information has been suppressed on grounds that it is 'business proprietary information' i.e. commercial-in-confidence. We submit that by seeking to play the important role of Accountability Agent in a co-regulatory scheme, designed to satisfy the public interest in effective privacy protection, applicants must be prepared to waive such claims in all but very exceptional circumstances. It is simply not acceptable for critical information that would allow an impartial assessment of an applicant's performance against the recognition criteria to be withheld.

Preamble

The effect of recognition of TRUSTe as a CBPR Accountability Agent (AA) will be to effectively 'privatise' compliance assessment and monitoring of US (and potentially other) businesses seeking to become APEC CBPR certified, presumably to gain a marketing advantage when offering services in other jurisdictions[2]. While the FTC will perform the Privacy Enforcement Authority (PEA) role in the

---

[1] Nigel Waters received the documentation as a stakeholder consulted by the Australian Government Attorney-General's Department. He has represented Privacy International at meetings of the APEC Data Privacy Subgroup. The analysis in this submission is by himself and colleagues from the Australian Privacy Foundation, but we are confident that the concerns we express would be shared by many other NGOs in member economies. We have not been able to establish if other economies have consulted representatives in civil society about this application for AA recognition.

[2] We note that at this stage, there is no sense is which CBPR certification confers any automatic recognition, exemption or dispensation on a business in relation to cross border data transfer obligations in any privacy law of any APEC member economy or of any other jurisdiction. However, the possibility that CBPR certification will be used in relation to cross border data transfers in future is an additional reason for caution in the granting

US, it has, like its counterpart PEAs in other jurisdictions, strictly limited resources, and can be expected to leave routine operation of the CBPR system in the US to TRUSTe, reserving its enforcement role to exceptional cases referred either by TRUSTe or by other parties.

In this context, all stakeholders in the APEC Privacy Framework have an interest in ensuring that TRUSTe's performance of the important AA role has both integrity and credibility.

While the JOP is satisfied that TRUSTe meets all of the recognition criteria and associated process requirements, we believe there are several matters that need to be clarified before APEC member economies indicate that they have no objection to TRUSTe being accepted as a recognised AA.

As well as the specific issues we have identified below with the JOP Report and TRUSTe's ability to meet the recognition criteria, we also submit that member economies need to take into account both some generic problems with trustmark or seal schemes and some specific documented problems with the TRUSTe scheme in particular.

One such problem is that TRUSTe is a service designed for online services. The trustmark is provided ONLY in relation to the online activities of the organisation. If the same organisation breaches privacy in another medium (e.g. telephone, mail, physical surveillance, human resources etc.) the trustmark is irrelevant. Complaints resolution will not be available, and the TRUSTe master services agreement specifically excludes activities that are not related to the specific website carrying the trustmark. This distinction has been used in the past by TRUSTe members to deny complaints.

We assume that TRUSTe would assert that its trustmark/seal programme, which it hopes will be recognised as 'CBPR compliant', makes no claim to cover all of the activities of a certified business, and that any misleading claim by a certified business to the contrary would be actionable under the FTC Act. However, we submit that consumers may easily be confused or misled into the belief that the APEC AA recognition applying to TRUSTe covers all activities of the relevant companies in circumstances that would either be outside FTC jurisdiction or too difficult to prove.

Comments on JOP Report

We note that while the legal entity behind TRUSTe is registered in Delaware (pp.4-5), the California Labor Code is referenced on page 7 because TRUSTe certification staff are located in California,. Does the dual jurisdiction give rise to any issues in relation to oversight of TRUSTe's participation in the CBPR system, including any limitations on the jurisdiction of the FTC in relation to TRUSTe operations?

Conflicts of interest (RCs 1-3)

The section of the JOP report on recognition criteria (RC) 1-3, concerning conflicts of interest, does not expressly address RC2, which deals with **business affiliations**. It is not clear how TRUSTe would deal with the situation of applications for certification from businesses which have a commercial interest in TRUSTe (or of complaints about such businesses if certified). TRUSTe's application contains brief discussion of how Directors would recuse themselves where necessary, but day to day CBPR matters are unlikely to be on Board agenda, and this does not address the obvious potential for operational staff to be influenced by ownership affiliations. We would expect the JOP to satisfy itself that TRUSTe has processes in place to deal with applications for certification from businesses with an ownership or other interest in TRUSTe.

Given that TRUSTe has been operating for many years, it would be relevant to know if TRUSTe has ever had a Director or Board member or significant owner / investor who is also a director or board

---

of AA accreditation. Each economy needs to consider whether the standards to be applied by an AA would provide sufficient protection for exports of personal data from their economy to that of the candidate AA.

member or owner of an organisation it certifies, and if so whether this potential conflict been clearly disclosed to the public or regulators?

TRUSTe has explained that is has internal arrangements to prevent conflicts of interest in relation to marketing and performing privacy **consulting services** separately from its certification and monitoring of CBPR compliance (TRUSTe' application (p.3) is contradictory as to whether it will in fact engage in such services). However, the detail of these arrangements, while supplied to the JOP, have been withheld from the JOP report on the basis that they are 'business proprietary information' (footnote 13). On pp 7-8 of its Report, the JOP does not expressly offer an opinion on the adequacy of these arrangements – we submit that there needs to be some discussion of this to assure member economies that the obvious potential for conflict of interest has been adequately addressed.

On the evidence of TRUSTe's public website, the distinction between its privacy seal program (TRUSTed Websites) and its privacy consulting services is far from clear.[3] Ambiguous references to the seal are followed by specific references to four categories of other services 'We Examine Your Privacy Policy'; We Scan Your Website for Potential Threats'; 'We Help You Align with Federal & State Requirements', and We Help You Resolve Disputes' (see also below on Dispute Resolution). These are presumably all commercial services separate from those directly associated with the privacy certification, and covered by the certification fee, whatever that is.

The JOP report states that TRUSTe will notify the JOP of any relevant consulting engagements – presumably any involving privacy advice or services not directly connected to CBPR certification, monitoring and dispute resolution (which would we assume be covered by a standard fee (see below). It is not clear that the JOP will have the capacity to receive and analyse notices of such engagements (potentially a high volume even from TRUSTe, with other AAs to follow), in which case the notices arguably serve no purpose.

The conflict of interest issue is so important that we submit 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.

Program Requirements (RC 4)

The recognition criterion requires an applicant to indicate if it has used the Annex C template to map its intake processes against the CBPR programme requirements, as an alternative to using the CBPR template Intake Questionnaire. While the completed map for TRUSTe has incidentally been the subject of detailed discussion by the APEC Data Privacy Subgroup – as an exemplar during the Pathfinder stage of its work – there is no documented process for a detailed assessment of the map by the JOP or any other party. We submit that it is necessary for the JOP to satisfy itself that an applicant's completed Requirements map is credible, and does not rely merely on assertions by the applicant.

In the Annex C 'map' attached to the application, TRUSTe has not given a YES or NO response to each question, but instead has merely inserted a column with quotes from their program documents. When these are examined, the answer to many of the questions is clearly NO, but there is no mention of this in the JOP report. In Attachment A to this submission, we give examples of cells in the Annex C table where we submit that TRUSTe's program standards/requirements do not appear to meet the CBPR program requirements. Our preliminary analysis is that, there are at least 21 of the APEC program requirements where TRUSTe 's program standards/requirements either do not include the APEC requirements at all (13/21), or fail to fully meet the APEC requirements (8/21). This compliance failure is far in excess of what member economies should tolerate as acceptable shortcomings by an AA. We emphasise that our analysis is not exhaustive, and there may be even more shortcomings.

---

[3] See http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-websites

Overall, it is very surprising that the JOP report states that TRUSTe has met the approval criteria, without any discussion or analysis of the many gaps and limitations in the TRUSTe program.

TRUSTe should be required to resubmit its application with a YES or NO for every question. Where the answer is YES they should provide evidence and examples. Where the answer is NO the applicant (and the JOP) should follow the procedures set out in the core requirements. This will often require the applicant to produce evidence of alternative processes etc. It is unclear why this has not been done in the current application. Any suggestion of suppression of information potentially unfavourable to an applicant – including on spurious commercial in confidence grounds, must of course be dispelled, if the credibility of the CBPR process is to be established.

Certification process (RC 5)

This criterion only requires a description of the AA's process, but we submit that it is implicit that the JOP should satisfy itself as to the **adequacy** of the process and its outcomes in terms of recognition. Otherwise, there would be no point in even requiring a description.

TRUSTe's process for certifying applicant businesses are summarised in the JOP report, but footnote 14 indicates that there is considerable discretion, on the basis of a TRUSTe assessment of the applicant's 'risk profile'.

We submit that it is impossible to make any assessment of the adequacy of TRUSTe's certification processes without more detail, and without knowing what scale of fees and charges will apply. Clearly the adequacy of the 'initial assessment', report, and any verification required (p 9) will depend on the resources TRUSTe applies and this will in turn, in this commercial model, depend on the fees charged. The level of fees paid must also be considered in light of potential conflicts of interests that can arise from payment of high fees. If the JOP has considered the TRUSTe business model in reaching its conclusion, this needs to be explained.

We also submit that the relationship between the various seals offered by TRUSTe (in particular TRUSTed Websites and TRUSTe PRIVACY SEAL) is not sufficiently clear in the application, and that the JOP should have required further information before concluding that the certification process, and its outcome, is adequate.

Ongoing Monitoring and Compliance Review processes (RCs 6&7)

AAs are required to monitor compliance by certified businesses on an ongoing basis. The JOP Report explains(pp.9-10) that TRUSTe proposes to do this using four mechanisms – web crawling, email seeding, traffic analysis and dispute resolution (the latter is separately required and discussed later). The first three are presumably automated processes, with human intervention only when 'exceptions' are reported by the automated tools. While allowing that this automated compliance monitoring goes well beyond what is in place under most existing privacy laws, it is not clear that it would detect breaches of all of the CBPR program requirements. As we have already noted, the focus of the TRUSTe privacy program on only the online operations of certified businesses does not sit comfortably alongside the requirement to meet all of the CBPR programme requirements including in relation to offline or back office processes.

There is surprisingly no reference in this section of the Report to referral of breaches to the FTC as the US Privacy Enforcement Authority (PEA), but this is covered later (p.14) – see comments below.

Re-Certification and Annual Attestation (RC 8)

RC 8 requires annual re-certification. The JOP report notes (p.10) that TRUSTe will '*investigate*' and if necessary '*verify*', in relation to recertification. Again, the adequacy of these processes can only be

assessed in light of the resources to be applied, which requires more information about the business model and fees.

TRUSTe has outlined three possible outcomes from a failure of certified business to satisfy TRUSTe about its continued compliance with the program requirements. These include, in extremis, 'referral to an appropriate authority' (p.10). We assume that this would include the FTC as the PEA, but question whether it is sufficient for this to be only a last resort after '*termination from TRUSTe's program*' and '*in extreme cases*'. We submit that there need to be clearly documented processes for much earlier referral of non-compliance to the FTC, in appropriate cases.

Dispute Resolution Processes (RCs 9&10)

The JOP Report summarises (p.11-12) TRUSTe's internal processes for dispute resolution. While these appear comprehensive, their effectiveness will again depend on resources. It is not clear whether TRUSTe will fund any dispute investigation and resolution from central sources or whether it will levy a charge on the respondent business. Again, more detail of the TRUSTe business model is required to facilitate an assessment of the adequacy of these processes, and the capacity of TRUSTe to provide an effective dispute resolution service .

It is not clear from the TRUSTe application, or from the JOP Report, what remedies a complainant could expect out of the dispute resolution process. It appears that TRUSTe cannot compel a certified business to pay compensation, make an apology, or undertake specific training or make any other specific changes in practices or documentation. Even if, as a result of an investigation, TRUSTe membership is terminated, TRUSTe has no ability to enforce other common privacy remedies, such as correction of data, removal of data and changes to practices. A consumer who has suffered a privacy breach may be no better off, and the suspension or termination of membership will not result in a positive privacy outcome for the affected individual.

We submit that there is insufficient evidence that TRUSTe will be able to meet the requirement of RC12 to be able to 'requir[e the] Participant to remedy the non-compliance within a specified time period' or the requirement of RC13 to impose '... Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent'.

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?

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. While not expressly specified in the AA Recognition Criteria, the need for such notice is implicit in the design of the CBPR system, whether an AA has chosen to provide dispute resolution 'in-house' or to contract it to a third party. If a candidate AA fails to include a guarantee of such notification in its processes, we submit that this must be regarded as a serious negative factor in its application, as a failure to sufficiently engage the PEA processes in its economy.

Mechanism for Enforcing Program Requirements (RCs 11-15)

The JOP report includes (pp.12-13) extracts from TRUSTe's Master Services Agreement (MSA) to illustrate how TRUSTe would enforce compliance with the CBPR program requirements, as required by RCs 11-15. The full MSA, while provided to the JOP, has been withheld from the Report on grounds that it is 'business proprietary information' (footnote 17). The extracts provided appear to be a sufficient basis for the JOPs satisfaction in relation to most of the processes. However, we submit that TRUSTe's declared criteria for referral to a privacy enforcement authority (PEA) do not fully meet Recognition Criteria 13(d) and 14. The threshold for referral summarised in the JOP Report (p.14 and footnote 19) are too high (e.g. only after termination) and leave too much discretion with

TRUSTe, including a subjective judgement about whether a PEA would be able to take action. TRUSTe's criteria seem to involve internal contradictions – if as they propose a decision to refer would involve consideration of '*factors such as whether the violation was egregious and intentional*' but only after 'termination' of certification, then this implies that they might terminate where the non-compliance '*impact was de minimis*', which seems unlikely.

We submit that it is also relevant to look at TRUSTe's history. TRUSTe has 4,000 members but appears to perform almost no enforcement activity. In a typical year only 5-10 members face either suspension or termination of the agreement. These are usually small organisations. There is no evidence that TRUSTe makes appropriate referrals to enforcement agencies – no examples have been provided by TRUSTe in their application and none are noted in their Transparency Report. This is despite the significant and well publicized privacy breaches by TRUSTe certified organisations such as Facebook, resulting in regulatory intervention and significant sanctions both in the US and elsewhere.

We submit that TRUSTe must commit to referral wherever 'such failure to comply can be reasonably believed to be a violation of applicable law' (RC 14) (as well as to notifying complainants of their right to complain directly to the PEA - see above).

We also submit that TRUSTe's commitment to '*where possible, ... respond to requests from enforcement authorities in APEC economies that reasonably relate to the CBPR-related activities of TRUSTe*' is far too weak and allows too much discretion and subjective judgement. In order to meet RC 15, TRUSTe must commit to a less constrained cooperation on request from the FTC, as the US PEA.

The application seems to suggest that TRUSTe operates in an environment where its commercial privacy products are part of a broader enforcement framework, based on a mix of FTC action and potential USPTO action (under the Lanham Act). We are not aware of any relevant action regarding trustmarks under the Lanham Act. The FTC has taken relevant action, on its own initiative, under the FTC Act, but this has often been against TRUSTe clients and in direct opposition to public statements of support by TRUSTe for its members – Facebook's many high profile privacy breaches are the obvious example here, as these are usually accompanied by glowing website stories about Facebook on the website truste.com.

Reporting (RC 10)

The JOP Report notes that TRUSTe proposes to comply with the public reporting requirements (RC 10 (g) and Annex E to the AA Recognition Application) by reference only to its annual Transparency Report. TRUSTe asserts that '*for purposes of anonymity, these case notes and statistics will be drawn from all TRUSTe-certified companies and not be limited to those companies that have received CBPR certification.*' We submit that this is unacceptable – it is essential that the CBPR compliance statistics be reported separately - otherwise the AA performance under the CBPR system cannot be independently assessed.

The TRUSTe Transparency Report contains no case studies, no critical analysis, and only very limited statistical information. For example, the largest categories of complaints that it reports are listed as 'other' or 'non-sensical'.

Case notes and statistics (RC 10)

TRUSTe also proposes to meet the case note requirement (RC 10(h)) by sending '*anonymised case notes to APEC member Economies*'. This is wholly inadequate. Provision of case notes 'in house' within member economies is not publication at all, which requires the case notes be available to the public. Publication, properly understood, contributes to the objective of helping to establish the credibility of the CBPR system to external observers (including those outside the APEC region), and

to informing both potential complainants (consumers and their advisers) and respondents (CBPR-certified companies, and potential members) what are the consequences of non-compliance, and what are the details of compliance as they play out in practical situations). Case notes are an essential 'feedback mechanism' in any credible system of regulation.

The Case Note FAQs included in Annex D to the AA Recognition Application make it clear that the intention is not only for casenotes to be published but for AAs also to facilitate third party re-publication as a contribution to the overall transparency and accountability of the CBPR system.

Overall transparency

It is very difficult to see how TRUSTe can meet the openness and reporting requirements in the AA criteria. TRUSTe is a secretive, commercial operation with proprietary products and procedures. They have never disclosed any information on referrals to regulators. They have never issued any negative case studies or even mild critiques for the large organisations that they certify, despite widespread and high profile breaches.

In the application, TRUSTe proposes to use its Transparency report to meet the APEC reporting requirements. This report contains no case studies, no critical analysis, and only very limited statistical information. For example, the largest categories of complaints that it reports are listed as 'other' or 'non-sensical'.

Conclusion

We submit that TRUSTe's application for recognition as a CBPR Accountability agent is manifestly inadequate and in several significant respects does not meet the required Recognition Criteria. We further submit that the entire TRUSTe business model makes it an inappropriate candidate for recognition as an AA. It's position as a candidate for the first accreditation as a AA is extremely unfortunate for the credibility of the CBPR process.

It is very disappointing that the JOP does not appear to have made a sufficiently thorough assessment of the application. From our own analysis of the application, we cannot understand how the JOP has reached its conclusions '*that TRUSTe has policies in place that meet the established recognition criteria and makes use of program requirements that meet those established in the CBPR system'* and that '*the conditions established in 6.2 (ii) of the Charter of the Joint Oversight Panel to have been met by TRUSTe'* and therefore its recommendation to *'... grant TRUSTe's request for APEC recognition ...*'

We submit that it is not appropriate for APEC member economies to make a consensus determination to accept the JOP Recommendation. Further information should be sought to address the many ways in which the application does not currently meet the Recognition Criteria, although we have no confidence that they can meet the Criteria.

Attachment A

Examples of cells in the Annex C table (Program Requirements map) where we submit that TRUSTe's program standards/requirements do not appear to meet the CBPR program requirements. We emphasise that this is not an exhaustive analysis

Question(s)	Issue	TRUSTe
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.)
3	Notice of 3rd part use	Not a TRUSTe program requirement
7	Lawful and fair collection	TRUSTe only requires activities to be lawful and not misleading. There is no test of fairness.
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.
22	Correction of inaccurate data	TRUSTe limits this requirement to 'commercially reasonable steps'. There is no discussion or analysis of this limitation.
23 and 24	Correction of inaccurate data to be forwarded to agents and relevant 3rd parties	Not a TRUSTe program requirement
25	Agents and 3rd parties to inform organisation regarding inaccurate data	Not a TRUSTe program requirement
29	Staff to be informed and trained re security policy	Not a TRUSTe program requirement
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.
35B (see also 47)	(Following transfer) 3rd parties must be required to promptly notify the organisation of a breach	Not a TRUSTe program requirement
37A	Steps to verify identity of persons seeking access	Not a TRUSTe program requirement
37B	Access to be provided within a reasonable time	TRUSTe allows initial period (30 days) to be extended indefinitely. No test of 'reasonable time'.
38C	Correction to be provided within a reasonable time	Not a TRUSTe program requirement
38E	Rights following refusal of correction	Not a TRUSTe program requirement
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).
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)
42	Initial complaints process to be 'timely'	Not a TRUSTe program requirement for its participants

Question(s)	Issue	TRUSTe
43	Explanation of remedial action	Not a TRUSTe program requirement
44	Staff training for compliance and complaints	Not a TRUSTe program requirement
47	Restrictions on 3rd parties undertaking further sub-contracting without consent	Not a TRUSTe program requirement
48	Verification of self assessments	Not a TRUSTe program requirement