April 2, 2012

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW. Room 4725
Washington, DC 20230

Via: Electronic filing: privacyrfc2012@ntia.doc.gov

Re: Docket No. 101214614–0614–01 – TRUSTe's comments in response to the Department of Commerce-NTIA's Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct

TRUSTe appreciates the opportunity to comment on the process being contemplated by the Department of Commerce's National Telecommunications and Information Administration ("NTIA") – to facilitate industry's development of consumer data privacy codes of conduct under the President's Privacy and Innovation Blueprint. TRUSTe supports the underlying framework of the President's Privacy and Innovation Blueprint – namely the Consumer Privacy Bill of Rights ("CPBR"). In fact, all of the principles represented by the CPBR are already reflected in our certification requirements.[1] TRUSTe also supports use of a Multistakeholder Process to determine privacy codes of conduct, but recommends that such a process include procedural safeguards to ensure that consensus is reached. The goal here should be the development of consumer privacy codes of conduct that industry will want to ultimately adopt and be governed by.

A. Scope of Issues

TRUSTe applauds the Administration and NTIA's efforts to bring stakeholders together - to develop industry codes of conduct that would extend the CPBR to commercial use of personal data not currently covered by existing federal privacy statutes. As a preliminary matter, we think it's important to define the scope that the codes of conduct are trying to address – including the types of harms the framework intends to address, and how these harms should be defined. We think that through the Multistakeholder process, this scope will be defined more accurately, creating codes of conduct that reflect the reality of commercial data collection and use today.

[1] See Chris Babel, How TRUSTe Powers Compliance with the Privacy Bill of Rights, available at: http://www.truste.com/blog/2012/02/23/how-truste-powers-the-privacy-bill-of-rights/

[2] TRUSTe examines how the client collects, uses and shares personal data; we also identify the client's third party, data-sharing relationships. See The TRUSTe Approach: Certification, *TRUSTe 2011 Transparency Report*, p.5. Available at: http://www.truste.com/resources/assets/TRUSTe-TransparencyReport-2011.pdf

In TRUSTe's own certification process, we look closely at data flows from the client's online product or service to determine whether our certification requirements are applicable.[2] A key trigger in our certification process is the collection of Personally Identifiable Information or "PII."[3] We also look at whether personal data is being collected in the business-to-consumer ("B2C") and/or business-to-business ("B2B") contexts. In doing so, we are able to impose obligations that are relevant to the data collection and use being contemplated.

This approach is also seen in compliance under other federal privacy statutes. For example, under the Gramm-Leach-Bliley Act ("GLBA"), a financial institution that collects and uses personal data is required to provide consumer notification of key changes around the collection and use of that personal data (including financial information) and how that personal data is being shared with affiliates and third parties.[4] The obligation is triggered by the creation of the relationship context. Further, where there is no personal data being shared, then there is no such notice obligation e.g. if anonymized or non-personal data is being exchanged between financial institutions. These data-flow driven obligations consider both context and sensitivity of personal information and as such, best manage the expectations of both the data subject and the entity using the personal information.

Because TRUSTe defines requirements around data flows, we are able to certify practices across a wide range of business models and technologies – with contextually relevant obligations that are based on the same set of certification requirements. We think that a similar approach may be used in the Multistakeholder process - to create codes of conduct that provide contextually relevant privacy obligations, while also bridging the various business models and technologies that comprise the online ecosystem today.

We note that the NTIA is considering an initial Multistakeholder process around providing transparency in mobile app privacy notices, and have provided some initial thoughts on this in section B. below. We would support the development of a code of conduct for mobile apps (which would also cover location-based services), as well as other topics mentioned in the NTIA's federal register notice (e.g. cloud computing services, the use of online technologies to store personal data, etc.). We would also support development

---

[2] TRUSTe examines how the client collects, uses and shares personal data; we also identify the client's third party, data-sharing relationships. See The TRUSTe Approach: Certification, *TRUSTe 2011 Transparency Report*, p.5. Available at: http://www.truste.com/resources/assets/TRUSTe-TransparencyReport-2011.pdf

[3] We define PII as "any information or combination of information that can be used to identify, contact, or locate a discrete Individual. See definition of Personally Identifiable Information ("PII") under TRUSTe's Program Requirements, available at: http://www.truste.com/privacy-program-requirements/program_requirements_website_privacy

[4] See generally, The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999 (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999).

of a code of conduct for Accountability, and have provided some additional thoughts on this point, and the Multistakeholder process in Sections C. and D. below.

B. Mobile Best Practices

TRUSTe believes that the principles embodied in the Consumer Privacy Bill of Rights can provide a foundation for consumer privacy on both the mobile platform and in mobile apps. TRUSTe's own Certification requirements – including those for our mobile certification program – reflect the CPBR principles.

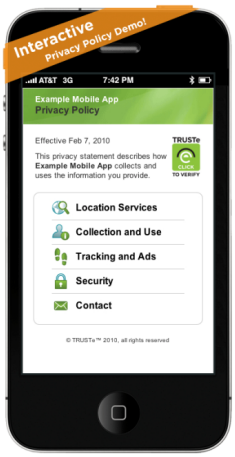
Included below are examples of how TRUSTe's requirements for mobile privacy notices already incorporate the principles of *Individual Control*, *Transparency*, and *Respect for Context*. We also provide some additional best practices that we think are relevant to the mobile content, and address how mobile notice may differ when marketing to children under 13 is involved.

1. TRUSTe Best Practice - Individual Control & Transparency

To fully give consumers Individual Control, they must have clear and transparent notification of the data collection at issue. Without Transparency of disclosure, an Individual cannot truly control her preferences regarding personal data collection and use. This challenge is intensified when presenting notice on the very small screen of the mobile device.

To address this challenge and develop privacy notices that are truly optimized for the small screen, TRUSTe has developed a standard representation of privacy practices and choices – using a mix of text and icons. The results are integrated into TRUSTe's mobile short notice format, which is implemented by clients under our mobile certification program. This short notice identifies the five categories of information that are most relevant to the mobile user: data collection and use, location data collected and use, tracking and ads, security settings, and contact information (see Figure 1, below).

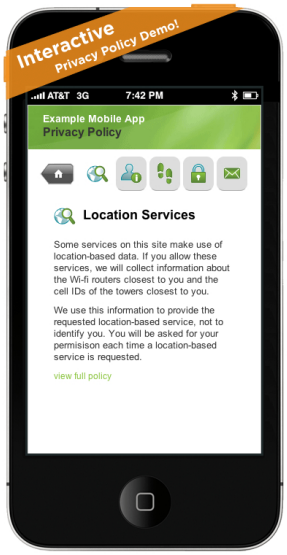
Figure 1 – TRUSTe Mobile Short Notice



2. TRUSTe Best Practice - Respect for Context

TRUSTe believes that Respect for Context, like Individual Control, is an important precursor to Transparency. Our mobile certification requirements - especially around the collection and use of location data - already embody the spirit of contextually appropriate notice. We recognize that location data can be captured by a wide range of devices – from desktop computers to mobile devices. However, we believe it is important to qualify the definition of geo-location data - to differentiate it from other types of location data.[5] In the case of a mobile device (which is inherently personal to begin with), the existence of GPS capabilities that can pinpoint the consumer's actual geographic location, intensifies the privacy risk. The challenge of course is keeping the user aware that their actual physical location is being tracked at any given point - without bombarding them with multiple notices that they might eventually turn off or ignore.

Figure 2 – TRUSTe Mobile Short Notice for Location-Based data



In such instances, TRUSTe requires that clients get express consent the first-time location data is collected, and provide additional notification, including just-in-time notices, when location data is subsequently collected and used. We are also experimenting with the use of persistent icons, and other reminders, so that users are constantly aware that location data is being tracked on their mobile devices.

[5] We define Geo-location Data as "Information obtained through an Individual's use of a Mobile Device and is used to identify or describe the Individual's actual physical location at a given point in time." See definition of Geo-location Data under TRUSTe's Program Requirements, available at: http://www.truste.com/privacy-program-requirements/program_requirements_mobile_privacy

3. Mobile Notice to Children under 13

One area of emerging importance is the requirements for mobile notice of apps and services directed to children under the age of 13. As NTIA knows, the legal requirements for such notice are set out in the Children's Online Privacy Protection Act or "COPPA," and the FTC has primary enforcement authority in this regard. TRUSTe has been an FTC-authorized COPPA safe harbor since 2001, and has witnessed several of the technological changes that are impacting compliance with COPPA (and necessitating the FTC's current review of the rule). We think some of these issues could be resolved within a Multistakeholder framework.

For instance, there are some practical issues when attempting to implement COPPA-compliant notice on a mobile device. The most significant is the "Multiple Operator Notice & Consent" problem. The current requirements of the COPPA rule provide an additional layer of complexity to mobile notice, especially in situations involving multiple operators. In its comments to the FTC's proposed changes to the COPPA rule, TRUSTe explicitly identified concerns around the "Multiple Operator Notice & Consent" problem, stating:

> The requirement of "…what information **each** operator collects…" will serve to continue to make notices an onerous document for parents to navigate, especially on a mobile device, as they try to figure out who each operator is and what it does with collected data. [6]

We think that this problem could be addressed through a Multistakeholder process that defines consent obligations under an industry code of conduct. Our view (as noted in our recent FTC comments) is that the consent obligation on the mobile platform should be limited to the primary operator. Any subsequent third party operators should be allowed to rely on the consent obtained from the first party operator where the third party is "operating" under the direction of the first party. In addition, we believe that a listing of multiple operators will confuse parents and complicate the operator's ability to obtain "verifiable parental consent" under COPPA.

4. Suggested Best Practice - Primary Notice

Consumers should be able to decide whether to install a mobile app, without having to first download the app to have access to the privacy policy. In such situations, a primary notice – providing highlights about what the software does (data collection and use, OBA, tracking) – can help a consumer make an informed decision about their purchase. An example of this is already seen in our certification requirements for the TRUSTed Download Program, which requires program participants to provide primary notice and access to other notices such as a privacy policy prior to the consumer consenting to installing the software.[7]

[6] See TRUSTe Comments to COPPA Rule Review, 16 CFR Part 312, Project No. P104503, available at: http://www.ftc.gov/os/comments/copparulereview2011/00231-82092.pdf

[7] TRUSTe, Program Requirements, 18 Nov. 2011, http://www.truste.com/pdf/Trusted_Download_Program_Requirements_Website.pdf.

5. Standardization of Mobile Privacy Notices

One potential area in the development of a mobile privacy code of conduct, that the NTIA could drive consensus around, is the standardization of terms used in privacy notices generally, and mobile privacy specifically. TRUSTe believes that increased standardization of terminology will assist in helping consumers understand privacy notices better. TRUSTe also believes that development of new terminology should not just be limited to words; as seen in our mobile short notice, we are already developing an icon-based system that provides a visual representation of privacy practices and choices. We think the standardization of mobile privacy notices that incorporate an icon-based nomenclature is particularly important given that the most consumers simply don't understand what's being said in a privacy notice. In fact, a recent review of the privacy policies of the top Fortune 100 companies found that on average, these privacy policies were drafted at the reading level of a junior in college, well beyond the general comprehension of the average US adult reader (who reads at an 8th grade reading level). [8]

C. Accountability

Accountability is a key part of TRUSTe's certification program and we hold our clients accountable for the promises they make in their privacy policies. We understand that Accountability can be an amorphous term that means different things to different organizations and jurisdictions. We view Accountability as the establishment of processes and controls for the purpose of holding the organization responsible and answerable for its actions in a manner transparent to those outside of the organization – consumers and other third party oversight organizations (e.g. regulator, auditor, Trustmark, or third party certification authority). While it is often presumed, TRUSTe believes that Accountability is an important component that should be explicitly defined and stated as part of an effective privacy code of conduct.

Furthermore, we think that Accountability has both an internal as well as an external component – and any definition of Accountability needs to encompass both elements:

a. Internal Accountability –We support the FTC's proposal that would require that companies maintain "comprehensive data management procedures throughout the life cycle of their products and services."[9] These should include internal data governance controls such as accuracy and data retention that are appropriate to the size of the business and the level of sensitivity of the data collected and stored.

b. Accountability to the Individual (Data Subject) – This type of accountability is particularly important for companies who build trust by holding themselves accountable to their consumers. Individual Accountability helps companies demonstrate that they are accountable to their consumers – not just through their internal controls, but also through their consumer practices. Often, Accountability to an individual will require that consumers be provided alternative forums and methods to express their privacy

[8] Paul Bond and Chris Cwalina, "Making Your Privacy Policy Comprehensive and Comprehensible," Corporate Counsel, 1 Sept. 2011, 18 Nov. 2011, http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202512963808.
[9] Protecting Consumer Privacy in an Era of Rapid Change, FTC Report, March 2012, available at: http://www.privacylawsalon.com/policymakers/2012/120326privacyreport.pdf

concerns. An example of this is TRUSTe's Dispute Resolution mechanism, which is part of our certification programs.

TRUSTe believes that Accountability can be incorporated into a code of conduct to ensure compliance. As an Accountability agent, we use a variety of approaches to monitor compliance. We monitor client websites with proprietary crawlers; we may also learn of non-compliance through consumer complaints received through our dispute resolution mechanism. If we find that our sealholders are out of compliance with TRUSTe's program requirements, we will initiate an investigation. Our client contracts include a number of enforcement provisions that are triggered when the client is not in compliance: suspension, termination and/or referral to a regulatory authority such as the FTC. Depending on the results of our investigation, TRUSTe will resort to one of these approaches for enforcement.[10] In this way, companies making public facing privacy promises about the consumer data they collect and use, are held accountable by TRUSTe for actions related to that consumer data.

It is our experience however, that most clients typically resolve issues before further action is necessary, because they want to remain with the TRUSTe program, and because they see the benefit of the TRUSTe seal to their business.[11]

D. Facilitating Participation in the Multistakeholder Process

TRUSTe supports the inclusion of all stakeholders in the development of consumer privacy codes of conduct – this is the only way to create a consumer privacy framework that is relevant for all participants in the Multistakeholder Process. The ultimate goal should be the creation of a code of conduct that industry will want to adopt because it makes both good consumer and business sense. Included below are some suggestions for encouraging broad participation in a way that is transparent, and reaches overall consensus.

1. Encouraging Broad Participation

Here are some specific ways to encourage broad participation by a wide range of stakeholders:

a. NTIA should communicate information about the Multistakeholder Process broadly across consumer and industry audiences – using social media and other tools to ensure distribution.

[10] For more details on TRUSTe's consumer dispute resolution and enforcement processes, please review our 2011 Transparency Report, available at: http://www.truste.com/resources/assets/TRUSTe-TransparencyReport-2011.pdf

[11] Two recent TRUSTe case studies highlight how eliminating privacy concerns can lead to increased online conversion rates. Displaying the TRUSTe seal led to a 13% increase in e-commerce conversion rates for the Baker Publishing Group. The full study is available at: http://www.truste.com/customer-success/baker-publishing/index.html. Online retailer Debnroo saw a retail conversation rate of 29% after displaying the TRUSTe seal. More details at: http://www.truste.com/customer-success/debnroo/index.html.

b. NTIA should set up a dedicated website that would provide resources and an online comment mechanism, designed to capture stakeholder feedback about the development of the consumer privacy codes of conduct, as well as the Multistakeholder Process. This is particularly important to encourage participation from stakeholders who aren't able to attend Multistakeholder meetings in person.
c. The NTIA should consider scheduling town hall meetings across the country to encourage "outside the Beltway" participation from consumers and businesses, especially those in the "tech corridors" – Austin, Boston, New York, Seattle/Portland and Silicon Valley.

2. Encouraging Transparency

In determining how it wants to be transparent about the Multistakeholder Process, the NTIA must also consider the need to foster an open and candid dialogue about the consumer privacy codes of conduct. In the age of instant media, stakeholders are even less likely to be candid and forthcoming on the public stage, than they would in a private meeting. The NTIA will need to consider this balance when determining, for instance, whether to webcast Multistakeholder Process meetings. Webcasting each and every meeting may actually chill the discussion and ultimately not create the Transparency the NTIA hopes to achieve with this process. However, it is also important that certain important meetings – where stakeholders debate the merits of their relative positions, or where key decisions are made – are memorialized either through a webcast or a transcript. Another way to ensure Transparency is requiring participants to submit a position brief or comments articulating their position on a particular issue, and posting these briefs on a Multistakeholder Process website in advance of any public dialogue on the issue.

3. Encouraging Consensus

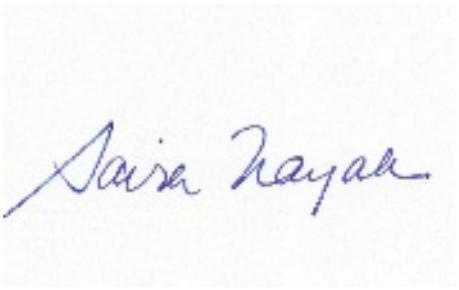
TRUSTe views overall consensus as a key driver to obtaining a code of conduct that industry will want to adopt. To achieve consensus, we suggest that the NTIA do the following:

- Establish and identify milestones for the Multistakeholder Process, including clear deadlines for debate around key provisions and the release of the final version of the code of conduct involved. Given that technology evolves quickly, we believe that the overall process to develop each code of conduct should take no more than 12 months to complete.
- Provide a draft for industry and consumers to review simultaneously, and a reasonable public comment period with options to provide online feedback. These drafts should be accessible electronically – preferably on the Multistakeholder website.
- Work with industry to establish a process by which the resulting framework may be updated in the future so that it is timely and relevant. For e.g. create a working group for the code of conduct at issue, with representatives from the consumer, industry and other stakeholder industries. This working group would meet regularly at set intervals, so that any technological developments can be reflected in the code's provisions in a timely manner.

TRUSTe appreciates the opportunity to provide comments on the process to define consumer data privacy codes of conduct under the President's Privacy and Innovation Blueprint. We support the principles outlined in the Consumer Privacy Bill of Rights, and believe that the Multistakeholder Process is an important way to implement this framework through industry-driven codes of conduct.

We look forward to working with the NTIA and other stakeholders on this important process.

Sincerely,



Saira Nayak
Director of Policy, TRUSTe