Fran Maier
President
fran@truste.com

February 18, 2011

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue N.W.
Washington, DC 20580

By Online Submission to: ftcpublic.commentworks.com/ftc/consumerprivacyreport/

Re: File No. 095416: Federal Trade Commission (Bureau of Consumer Protection) – Staff Report: *Protecting Consumer Privacy in an Era of Rapid Change*

TRUSTe welcomes the opportunity to comment on the Federal Trade Commission's Staff Report ("FTC Report"), *Protecting Consumer Privacy in an Era of Rapid Change*. TRUSTe has helped businesses build consumer trust and achieve online privacy compliance since 1997. We work directly with both consumers and businesses, expertise that gives us a unique perspective on the issues identified in the FTC Report.

Currently, TRUSTe certifies the online privacy practices of over 3500 web properties across a variety of platforms and services.[1] Our diverse client base includes companies of all sizes and industries, from small e-commerce websites (Featherplace, Koya Project) to major pharmaceutical companies (Pfizer, Merck), as well as top online brands like Apple, eBay, and Microsoft. One aspect of TRUSTe privacy certification is that companies must agree to ongoing participation in our Dispute Resolution Program, which allows consumers to file privacy complaints against our licensees. TRUSTe works hand in hand with the complainant and our sealholder to resolve the issue, and in 2010 we resolved over 7,500 such complaints.

TRUSTe knows that the FTC Report will be highly influential in establishing the direction of consumer privacy for many years to come. The Report's publication comes at a time when the online landscape continues to evolve at a dynamic pace. Innovative technologies - behavioral targeting, geo-location and social networking to name a few – are rapidly transforming the way we communicate, while also highlighting the need for better privacy protections online. TRUSTe has observed these changes in the online landscape closely, working with clients to resolve the privacy challenges arising out of some of these newer business models. We've also commenced an internal review of our privacy seal program requirements, and based on this review, plan to release revised program requirements in Spring 2011. We are particularly pleased to see that our internal thinking on many key updates to our privacy seal program requirements –

[1] TRUSTe – Trusted Sites, available at: http://www.truste.com/trusted_sites/index.html

particularly around the important concepts of choice and transparency - are in line with the proposed framework outlined in the FTC Report.

EXECUTIVE SUMMARY

To summarize our main comments on the FTC Report:

Scope - TRUSTe believes that the FTC should consider three factors when determining whether a practice falls within the scope of the proposed framework: the context of the transaction, the harm to be avoided and the proportionality of the regulation being imposed. Furthermore, we support the Commission's recognition of the diminished importance of statically defined personally identifiable information ("PII"), in a world where a number of combinations of data elements can be used to uniquely identify a user.

Privacy by Design – TRUSTe understands the importance of Privacy by Design (incorporating privacy protections at the product level) and is pleased to find support for this principle in the FTC Report. We believe that to be successful, Privacy by Design must incorporate two additional Fair Information Privacy Practices: Access and Accountability (both internally and to users). We see Access as a critical part of empowering consumers to participate more fully in the online data ecosystem. In addition, we see Accountability as proactively reducing the possibility of a privacy threat instead of merely providing redress once that threat has materialized.

Simplified Choice – TRUSTe applauds the inclusion of "Simplified Choice" as a building block of the FTC Report's privacy framework. Many of TRUSTe's recent innovations in consent mechanisms – Short Notice, Just in Time Notice, and Mobile Notice – reflect the position expressed by the FTC Report i.e., choice should be offered at the time and in the context in which the consumer data transaction is taking place.

Greater Transparency – We support the Commission's recognition of the need for Greater Transparency in privacy notices - such as the use of well-accepted terminology, icons and other guideposts in privacy notices - to increase consumer understanding and facilitate informed choice. We also support the use of machine-readable privacy policies, as they are a more accurate way of ascertaining the actual privacy protections of a web site or service.

Included below are detailed responses to specific questions listed in Appendix A of the FTC Report.

A. SCOPE

The FTC's proposed framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or device.

As a general comment, TRUSTe supports consideration of three factors when considering whether or not a practice falls within the scope of the FTC's proposed privacy framework:

- **Context** – We believe that any rules around disclosure should be crafted in a way that considers the context and privacy expectations of the transaction.

- **Harm** – We think that harm is an important part of the scope analysis. We support the Commission's recognition of non-economic or intangible harms - such as reputational harm - as well as financial harm, for purposes of redress, but recognize that this may present definitional challenges.

- **Proportionality** – When determining scope, we also think that it is important to consider whether the privacy rule being imposed is appropriate to the size and complexity of the practice being regulated.

In these comments, we have referenced these three factors – Context, Harm and Proportionality – where appropriate; we have also included references to specific implementations of this analysis in TRUSTe's privacy seal requirements (both current and proposed). We believe that application of these three factors will enable a privacy framework to balance the sometimes-conflicting needs of consumers and business. We note that the Commission has already adopted this approach in its discussions around data sensitivity and "commonly accepted practices."

TRUSTe also supports the Commission's recognition of the diminished importance of statically defined PII, since a combination of discrete data elements – while lacking identifying characteristics on their own - can be used in combination to personally identify a consumer. In our updated privacy seal program requirements, we adopt a revised definition of PII that incorporates this understanding.

3. ***Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?***

In addressing Scope, TRUSTe will address privacy issues related to "covered entities" separately from those related to "consumer data."

TRUSTe supports the inclusion of all commercial entities that handle consumer data within the FTC's proposed privacy framework. We believe that this in line with an appropriate understanding of the term "consumer" under both the current expectation of

a data subject as well as §5 of the FTC Act. By defining Scope in this manner, the Commission has heightened the importance of considering Context when determining the privacy impact of a particular business practice. For instance, many businesses that use "commercial consumer" data do so without any direct contact with the data subject.

It is TRUSTe's view that all entities that possess and use consumer data about an individual should be included within the FTC's privacy framework. We note for instance that certain entities e.g. non-profits, have access to consumer data, but would be excluded from the framework as currently articulated in the FTC Report because they are not considered a "commercial entity." TRUSTe would support the application of the FTC's privacy framework to all entities that possess and use consumer data, regardless of whether they are a commercial entity or not.

4. Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer or other device?"

TRUSTe is concerned that by qualifying Scope using the language referenced above i.e. all "data that can be reasonably linked to a… computer or other device, " the FTC Report makes the scope of the proposed framework unreasonably broad. For instance, this definition would include data residing in server logs about computer-to-computer communications – data that cannot be linked to a specific individual**.** An analysis of Context, Harm and Proportionality are particularly important here to avoid imposing a use limitation on data that has no connection to an individual person. To remedy this, TRUSTe would recommend making two important changes to the above-referenced portion of the Scope definition:

i. Change the word "or" to "and" between "consumer" and "computer or other device".

After this revision, the framework's Scope would only apply to consumer data that can be "reasonably linked to a specific consumer and computer or other device," i.e. consumer data linked to a specific device must also be linkable to a specific person. This would cover data collected from multiple sources and still only impose a privacy duty where such data can be linked to a person as well as the device. Since the FTC's focus is the mitigation of consumer (not web-server) harm, it should impose a privacy obligation only when there is a nexus between the individual and a particular device.

ii. Include Context and Harm language in the statement.

TRUSTe would also recommend including additional language to address Context and Harm, while also removing the ambiguous concept of "reasonableness" from the Scope definition. Harm would be addressed in the specific obligations surrounding the data and its sensitivity.

The revised portion of the Scope definition would then read as follows:

"…consumer data that is or will be linked to a specific consumer and computer or other device, where such data can be used to harm the specific consumer."

5. How should the framework apply to data that, while not currently considered "linkable," may become so in the future?

Data may not be "linkable" at the time of its collection, however, if the intent is to link the data with other data at some point, then the Commission should define the criteria by which such collection should fall within the scope of the FTC's proposed privacy framework.

B. PRIVACY BY DESIGN

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

As a general principle, TRUSTe supports the Commission's articulation of "Privacy by Design," and the importance of integrating privacy protections into a product's development life cycle. We recognize that companies may use Privacy Impact Assessments or "PIAs" to help identify privacy issues during product development. In our view, PIAs are a risk management tool usually used to help companies identify and manage risk *after the fact*. With the short development cycles of web products and services today, this is an approach that could result in additional cost, especially if privacy protections are being integrated after the product has been created. The better approach - and one that is more scalable across businesses of all sizes – is to build privacy into the product lifecycle from the start rather than considering it "after the fact." TRUSTe believes that this is the approach that better matches the agile product development life cycle that is characteristic of so many innovative companies today.

1. Are there substantive privacy protections, in addition to those set forth in Section V(B)(1) of the report that companies should provide?

TRUSTe supports the inclusion of two other substantive privacy protections into the FTC Report's privacy framework: Accountability and Access.

i. Accountability

We believe that Accountability should be included in the FTC's articulation of Privacy by Design. TRUSTe understands that Accountability can be an amorphous term that means different things to different organizations and jurisdictions. Fundamentally, Accountability is the establishment of processes and controls for the purpose of holding the organization responsible and answerable for it's 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).

As the Commission well knows, Accountability is a cornerstone of a robust global privacy framework such as APEC, or the OECD. While it is presumed, TRUSTe believes that Accountability is an important component that should be explicitly defined and stated as part of an effective privacy framework.

TRUSTe observes that Accountability includes both internal controls as well as external responsiveness to the data subject. Any definition of Accountability needs to encompass both elements:

> *a. Internal Accountability* – TRUSTe views internal accountability as the mechanism that verifies whether a company is complying with data controls and policies. We support the FTC Report's recommendations that companies dealing with consumer data should have internal data governance controls such as accuracy and data retention. These controls should be 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 the Individual will require that consumers be provided alternative forums and methods to express their privacy concerns.

Companies implement Accountability in many different ways. One method is providing a publicly accessible privacy policy that provides transparency and holds the company accountable to their own representations i.e., "do what they say, and say what they do." Under TRUSTe's privacy seal program, Accountability is tied to a standard of practices that companies must describe in their privacy notices and comply with in actual business practice as well as meet their own representations.

To hold clients accountable for the promises they make in their privacy policies, TRUSTe uses a variety of approaches. We monitor sealholder 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 sealholder contract includes a number of enforcement provisions that are triggered when a sealholder 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.[2] In this way,

[2] In September 2008, TRUSTe terminated its privacy certification of Classic Closeouts, after the company violated several of TRUSTe's program requirements around collection and use of consumer data and data governance. TRUSTe promptly suspended Classic Closeouts after first hearing numerous consumer complaints about unauthorized and unreimbursed charges. When Classic Closeouts refused to meet the necessary obligations to reinstate its sealholder status, TRUSTe expelled the company from its privacy seal program. TRUSTe also helped over 200 consumers resolve outstanding disputes by managing and handling

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. Most sealholders, however, are eager remain with the TRUSTe program and will typically resolve issues before further action is necessary, because they see the benefit of the TRUSTe seal to their business.[3]

ii. Access

TRUSTe applauds the discussion of Accuracy as a substantive element of privacy protection in the FTC Report. We believe however, that the discussion needs to be taken one step further, and that Access should be included as a requirement in the framework to ensure that any consumer data that is collected is timely, relevant, and accurate. The Access requirement should especially be considered in cases where inaccurate information could result in a negative outcome for the consumer.

It is TRUSTe's position that both the context under which data is collected and the purposes for which companies intend to use the collected data, will drive the level of Access companies are required to provide. This means that the mechanism by which Access is offered should correspond to the type and level of sensitivity of the collected data; it should also be appropriate to the size of the company that is collecting the data.

Access is an important part of TRUSTe's privacy seal program requirements. In general, TRUSTe's access requirements are in line with those required under the Safe Harbor agreement between the United States and the European Commission. All TRUSTe seal holders are required to offer access and control of data to consumers for the purposes of correcting inaccuracies or updating information. Basic requests, such as a complete opt-out, and/or removal of personally identifying information data from use, must be offered by TRUSTe certified sites at no charge to the consumer. For unusual requests that require the utilization of more internal resources, Access must still be offered, but the consumer can be charged with a reasonable fee for the service.

In addition to requiring access for the purposes of correcting inaccuracies or updating information, TRUSTe is moving towards a requirement that all sealholders also provide mechanisms for deletion or de-activation of data if so desired by the consumer.

Companies that offer Access should be recognized – not only for the transparency of their privacy practices, but also for enabling their consumers to make informed

---

consumer complaints, and in some cases, helping to obtain refunds from irregular charges that were incurred on the Classic Closeouts Web site. See, TRUSTe Helps Hundreds of Consumers Recover Refunds from Online Retailer, September 23, 2008, available at: http://www.truste.com/about_TRUSTe/press-room/news_truste_helps_consumers_recover_funds_from_retailer.html

[3] 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.

decisions about privacy protections. The Commission should also consider the important role of trusted third parties to certify the accuracy of posted privacy policies. Trusted third parties already serve an important role in other successful compliance schemes e.g. the PCI (payment card) data compliance system.

2. Is there a way to prescribe a reasonable retention period?

TRUSTe believes that while sites should publicly state their data retention policies, there is no way to prescribe a reasonable retention period for consumer data across all the different sites (and business models) that comprise the online data ecosystem. In addition, state safeguards and disposal laws differ in terms of how long data must be retained. While it is possible to design a retention period around the longest retention period required under state law, this approach may be unworkable, and may result in companies retaining data for longer than is necessary. For instance, in some cases, data cannot be retained if the consumer withdraws consent for its use.

Furthermore, companies may be obligated to keep certain information for a longer period of time to comply with law enforcement requests. Finally, companies must consider the cost of maintaining and securing consumer data – a cost that increases with the length of the data retention mandate. For all of these reasons, it would be difficult to prescribe a universal reasonable retention period for the collection of consumer data.

3. *Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that the retention periods for such data can be quite short?*

It is TRUSTe's position that data should not be kept longer than is commercially reasonable or required by law. However, when crafting a data retention period, regulators should consider the context of the particular data transaction, the harm to be addressed, and the proportionality of the retention mandate to the practice being regulated. This means that retention periods will differ depending on the context of the transaction and the legal rules around use of the consumer data being collected. TRUSTe also believes that use limitations and purpose restrictions are important to address the privacy concerns around data retention.

C. SIMPLIFIED CHOICE

Simplified Choice – Companies should simplify consumer choice.

1. What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?

The most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category is to look at the Context of the practice – what type of

data is being collected and with whom is it being shared? By identifying a spectrum of consent depending on the Context, companies can identify the appropriate level of protection for each data use scenario.

Sensitive data that is collected for first-party use must require a consumer's express consent before it is shared with third parties. This notice can be implemented through a variety of technologies: a check box at the point of collection, a scroll over, or a Just-in-Time notice provided in addition to a link to the privacy policy. Furthermore, unique notice must be given at the point of collection for each piece of data, detailing what is being collected and with whom it will be shared.

For non-sensitive data collected only for first-party internal purposes, the current regime of implied consent is still appropriate; it presumes that notice – through a company's privacy policy - is available for the consumer to review at any time. For non-sensitive data that will be shared with third parties, a consumer must be given notice that the data is going to be shared - either through a link to a privacy policy at the point of collection, or a check box at the point of collection.

Under our updated privacy program requirements, TRUSTe sealholders are required to provide a Just-in-Time notice, along with an opt-out mechanism, if the client shares PII with third parties for unexpected purposes. TRUSTe recently surveyed 100 of its sealholder web sites and found that 95 percent of the surveyed sites provided this type of heightened notice at the point of PII collection. TRUSTe requires that companies disclose the types of companies a consumer's PII is shared with – but does not require the identification of such third parties by name. The reason for this is that business relationships between companies change and evolve over time. Some relationships are for a short period of time which makes it difficult as well as costly for businesses to effectively disclose which third parties PII is being shared with. We have found that providing an effective choice mechanism is an approach that both enables companies to effectively build consumer trust and manage the costs of doing business.

An example of obtaining consent for new functionality is TRUSTe's Trusted Download Program. Under the requirements for this program, seal holders must provide a Just-in-Time notice when new functionality is added after the Individual has consented to the initial installation of the software. Figure 1 below is an example of a Just in Time notice presented by the ALOT toolbar after the toolbar is installed but before the "ALOT Discover" functionality is installed on the user's computer. This Just in Time notice communicates that ALOT Discover tracks a user's behavior online and requires the user's affirmative opt-in to enable the functionality (no default option is pre-selected).

Figure 1 – TRUSTe Just in Time Notice Format

2. Should the method of consent be different for different contexts?

Choice options and mechanisms should be flexible and relevant to the context of the data being collected and the platform being used. On a traditional website viewed from a desktop or laptop computer, longer-form consent events such as traditional privacy policies can still play a role, but these privacy policies alone are insufficient to make informed choices. A short notice is needed at the point that consumers make privacy-related decisions. Consumer educational efforts such as Privacy Information Centers, which explain a company's privacy policies in detail, can also assist the consumer in understanding the privacy impact of a particular practice.

Providing choice on mobile and other smaller-screen platforms presents different needs and challenges. These challenges can be addressed through the use of Short Notice, which facilitates notice in a limited space. Choice on the smaller screen can also be facilitated through the use of unique privacy icons. TRUSTe supports the creation of privacy icons, which we view as especially useful in this context.

TRUSTe also supports the use of just-in-time notices in the mobile application context (such as those currently seen on Android or iOS); for example, a pop-up window warning consumers when applications are sending geo-location data (which could be considered Sensitive data) to a Third Party.

3. Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

Please see our answer to question 4. in this section.

4. ***What types of disclosure and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services? In particular, how should companies communicate the take it or leave it" nature of a transaction to consumers? Are there any circumstances where a "take it or leave it" proposition would be inappropriate?***

TRUSTe believes that most eCommerce transactions can be conducted on a "take it or leave it" basis. This will give businesses the ability to innovate and control their own business practices. The notable exceptions would be transactions in certain highly regulated sectors such as Financial, Medical, Internet Service Providers, etc. These organizations are already heavily regulated regarding consumer education and choice. For other businesses, the "Take it or Leave it" approach can be used without harm to the consumer so long as there is clear notice, the use is within the company's primary purpose, and there is a way for consumers to request that their data be removed from use. While a business should be able to use the "Take It or Leave It" approach, the consumer needs to know that they can "Leave It".

Companies currently communicate the "take it or leave it" proposition through densely written privacy policies. TRUSTe believes that these policies should either become shorter and more articulate, or that the "take it or leave it" proposition should constitute a prominent layer of an effective multi-layered approach to privacy notice. A short notice, providing specific information on the nature of the business, and how the business utilizes a customer's data, would constitute one of these layers.

TRUSTe also believes that use of a Just-in-Time notice, provided at the point that the user signs up for the service, would educate consumers about the "take it or leave it" nature of a service and provide enhanced user choice.

If the "take it or leave it" proposition is in the context of a material change to an existing service, a prominent notice must be provided to allow users to leave the service. TRUSTe requires that in instances where there is a material change to a service, that the company provides prominent notice *before* the material change goes into effect, so that consumers have the opportunity to request that the company no longer use their information.

5. ***How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?***

TRUSTe agrees with the Commission that the definition of Sensitive information should include information about children, financial and medical information, and precise geo-location data. However, TRUSTe thinks about "Sensitive Information" in terms of the harm caused; information whose unauthorized disclosure or use can cause financial,

physical, or reputational harm is considered “Sensitive Information” under TRUSTe’s privacy seal program requirements.

TRUSTe agrees that consent should be required to obtain sensitive data. We believe that using any sensitive information, for purposes beyond which the information was originally collected, should require the express consent of the consumer through a separate consent mechanism. In addition, businesses should provide a just-in-time notice either right before or at the point of the sensitive data collection. We note however, that it is still common practice for businesses not to obtain the individual’s affirmative consent before sharing sensitive information. Further, to obtain true affirmative consent, appropriate notice and education should be provided so that the consumer can make an informed decision.

Grouping sensitive users is more difficult to define and handle. Various laws already define some groups of sensitive users e.g. the Children’s Online Privacy Protection Act (“COPPA”), which aims to protect children online. However, to identify other sensitive groups, such as those with mental illness, a site would have to collect more personally identifiable information than is necessary to conduct most transactions, just so that they can identify which sensitive group an individual may fall into. TRUSTe believes that businesses should follow principles of good data governance and not collect any more data than necessary. Thus we recommend, similar to current COPPA requirements, that businesses only identify users as members of sensitive groups when their business purpose specifically requires that information.

As for whether teens should be considered a sensitive group of users, we point to our Fall 2010 study of parents' and teens' social networking habits, entitled "The Kids Are Alright" (full survey results and material are available here.) Our survey found that 80 percent of parents and 78 percent of teens felt in control of their personal information on social networks, while 72 percent of parents actively monitored their teen's social networking activity. While these are positive findings, our survey did uncover areas where parental oversight and teen familiarity with privacy controls did not stop teens from exercising poor privacy judgment online. Specifically, we found that 68 percent of teens surveyed had at some time accepted online "friend" invites from strangers and 18 percent of teens had been embarrassed or disciplined as a result of sharing information on a social network. Our recommendation then, as we articulate in our new program requirements, is to obtain the teen’s express consent prior to allowing the teen to disclose or otherwise share information about themselves or other teens on their social network profile page.

6. Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

At minimum, TRUSTe believes that data brokers should provide consumers with an easy, accessible way to have their data removed from widely available mechanisms for general publication. In crafting a standard opt-out for data brokers, TRUSTe would encourage consideration of the following:

- Use of a persistent opt-out as is commercially reasonable
- Careful drafting of applicable use limitations
- Requirements that encourage companies to delete the information once the consumer exercises the opt-out.

7. What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?

The FTC Report outlines a " Do Not Track" initiative that would offer a standardized, uniform way for consumers to control how they are being targeted by advertisers based on prior online behavior. TRUSTe supports "Do Not Track" as one of many tools that can be employed within a self-regulatory strategy, in fact we recently announced our participation in providing a Tracking Protection List for Internet Explorer 9.[4] We believe that an excessive focus on "Do Not Track" technology or a "Do Not Track" list could take away momentum from promising self-regulatory efforts to provide consumers with ad privacy notice and choice.

One concern is that "Do Not Track" technology-only implementations may actually produce more opaque online tracking practices designed to circumvent these implementations. We've seen this outcome before - most recently, when advertisers used "locally stored objects" (a.k.a. Flash cookies) instead of traditional HTTP cookies to track an individual's web behaviors over time. Advertisers made this switch because browser-based "Erase Cookies" commands did not, in most cases, erase Flash cookies.

TRUSTe believes that online advertisers and trackers can and will find ways to work around pure technology solutions unless these technologies go hand in hand with self-regulatory frameworks that bring monitoring, verification and accountability into the picture. One way to achieve this is through third-party accountability agents, like TRUSTe, who work with both companies and consumers to ensure that transparency, accountability and choice exist in the online advertising ecosystem.

Toward this end TRUSTe has developed TRUSTed Ads, a self-regulatory technology platform that allows advertisers and publishers to serve accurate and scalable ad privacy notice and choice regarding Online Behavioral Advertising across billions of ad impressions. Consumers surfing on Web pages or viewing ads where TRUSTed Ads has been implemented can click on the Advertising Option Icon or other representation to find out which companies are involved in tracking on the page or for a specific advertisement or for a specific publisher. TRUSTed Ads then offers these consumers the choice to exercise a blanket opt-out of tracking or a granular opt-out on a company-by-company basis. TRUSTe also supports TRUSTed Ads by providing consumers with a mechanism for feedback or complaints.

---

[4] TRUSTe's TRUSTed Tracking Protection List for IE9, hosted at www.attrackingprotection.truste.com, is designed for the average consumer who has little to no expertise in the advertising ecosystem. See also, Kevin Trilli, TRUSTe TPL: Next Steps, available at: http://www.truste.com/blog/.

In a six-month test of TRUSTed Ads with PCH Lotto in 2010 we found that just over 1 percent of consumers who engaged the preference manager, after being presented the TRUSTe icon and education, chose the blanket opt-out.[5]

The low opt-out rates observed by TRUSTe and others might seem counterintuitive and suggest to some that consumers don't, in fact, care about online tracking. Instead, we believe they suggest that consumers want to understand what's going on with their information and have the option to exercise control – even if they don't necessarily exercise that control. In the test of TRUSTed Ads, over 55% of consumers indicated that the TRUSTed Ads experience was "helpful."[6]

Finally, it's important to remember that online tracking not only allows companies to serve more targeted and lucrative ads, but also allows them to provide consumers with enhanced, personalized browsing experiences; such as automatically showing consumers weather reports for their local area; remembering their preferred volume setting on a video website; or the contents of their online shopping cart.[7] Consumers need to be educated that blanket opt-outs of online tracking could negatively impact their online browsing experience outside of advertising contexts.

D. GREATER TRANSPARENCY

Transparency – Companies should increase the transparency of their data practices.

1. What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

TRUSTe believes that increased standardization is required across privacy notices so that consumers can make informed choices. The Commission should be careful however, to provide guidance rather than a prescriptive standard for notice – to balance the need to provide informed consent, with the need to innovate across multiple business models, platforms, and approaches.

A potential drawback to comparative privacy notices is that consumers may misconstrue the context under which data is being collected. This could further confuse or mislead consumers, as they compare privacy practices between different companies, and across different platforms. Also, comparative notices may not adequately address practices that are unique to emerging and evolving business models e.g. marketing to users based on geo-location data.

---

[5] Fran Maier, Presentation on TRUSTed Ads, November 2010, available at: http://www.truste.com/pdf/TRUSTe-OBA-Behavioral-Advertising-Opt-Out.pdf
[6] Fran Maier, Presentation on TRUSTed Ads, November 2010, available at: http://www.truste.com/pdf/TRUSTe-OBA-Behavioral-Advertising-Opt-Out.pdf
[7] Fran Maier, Presentation on TRUSTed Ads, November 2010, available at: http://www.truste.com/pdf/TRUSTe-OBA-Behavioral-Advertising-Opt-Out.pdf

TRUSTe also recognizes that consumers may interact with a company though multiple platforms and that one standard notice format may not be effective on all platforms e.g. a comprehensive privacy policy reads better on a desktop computer screen than on a mobile device screen. Increased standardization of terminology will also assist in helping consumers understand privacy notices, because the terms will be consistent in all forms of the privacy notice. TRUSTe also believes that development of new terminology should not just be limited to words; we are currently exploring the use of icons that can provide a visual representation of privacy practices and choices.

Under our new program requirements, TRUSTe has developed alternate forms of notice that exist outside of the traditional full-length privacy policy, defining them as part of the "Privacy Statement." These include:

- Short notices, i.e., a summary of a company's privacy policy and practices that is consistent with that company's privacy policy.
- Just-in-time notices, i.e., notice that describes a use or practice that is not already described in the company's privacy policy. Just-in-time notices are recognized as a way for companies to provide timely and relevant notice, especially at the point of collection for sensitive data.
- Mobile Notices - For notices on mobile devices, TRUSTe focused on using a mix of text and iconography to create an effective, intuitive, and easy-to-read layered notice. By doing so, TRUSTe addresses privacy issues relevant to a consumer's interaction with the company through a mobile device e.g. the collection and use of geo-location information.

2. How can companies present these notices effectively in the offline world or on mobile and similar devices?

TRUSTe acknowledges the widespread recognition that privacy statements currently do not provide the level of transparency needed for consumers to make informed privacy choices. Consumers should not have to read through lengthy privacy policies to understand how a company will use their personal or sensitive data, and what choices they have over the use of that data.

Some in the privacy community have proposed alternative privacy notices modeled after food nutritional labels. While this approach compartmentalizes privacy practices and in theory allows privacy comparisons to be readily made across websites or companies, the contextual nature of privacy makes this a problematic model for consumer notice. Whereas "Vitamin C" is "Vitamin C" whether it is found in an apple or an orange; a privacy disclosure concerning "the use of third-party tracking cookies" can have a very different meaning for consumers on a social networking website than it does on a banking website. Seeing how the context of information sharing can substantially impact consumer privacy, we should focus on the adequacy and readability of privacy disclosures rather than trying to identify unifying privacy metrics that produce unbalanced comparisons void of context.

Consumers care about the fundamental elements of privacy – what data is being collected, how that data is being used, and what Choice mechanisms are being provided. For the most part however, privacy notices are long and difficult for the average consumer to understand, and many consumers do not read them. When consumers do read privacy policies they may not always understand them – since the terminology can differ from one privacy statement to another. It is unlikely, however, that the full length privacy policy will disappear; we think that it will likely remain as the foundation for other forms of privacy notices, especially layered notices.

To solve the privacy notice problem, TRUSTe recommends a multi-pronged approach:

- Identify whether the business practice involves a common use case or a specific notice and choice mechanisms – don't "boil-the-ocean" in trying to solve the whole problem at once.
- Utilize a mix of innovation and standardization when determining the accessibility, presentation and readability of the notice. For example, some companies utilize videos that explain privacy practices and highlight tools. By "putting a face on privacy," these companies help consumers manage their privacy preferences.
- Improve privacy notices in a way that is scalable across businesses of all sizes. A "Short Notice" for instance, can be very effective in summarizing a company's privacy practices. Short notices work in tandem with a company's comprehensive privacy notice (something more and more companies have), providing consumers a snapshot of the company's practices and allow consumers to easily locate mechanisms for exercising Choice and requesting Access. Short notices can work within a variety of form factors such as web and mobile.

In a recent review of 100 client sites, we found that 25% of those sites were moving to a short notice format. In fact, TRUSTe is working towards short notice adoption by the majority of its seal holders by December 2011.

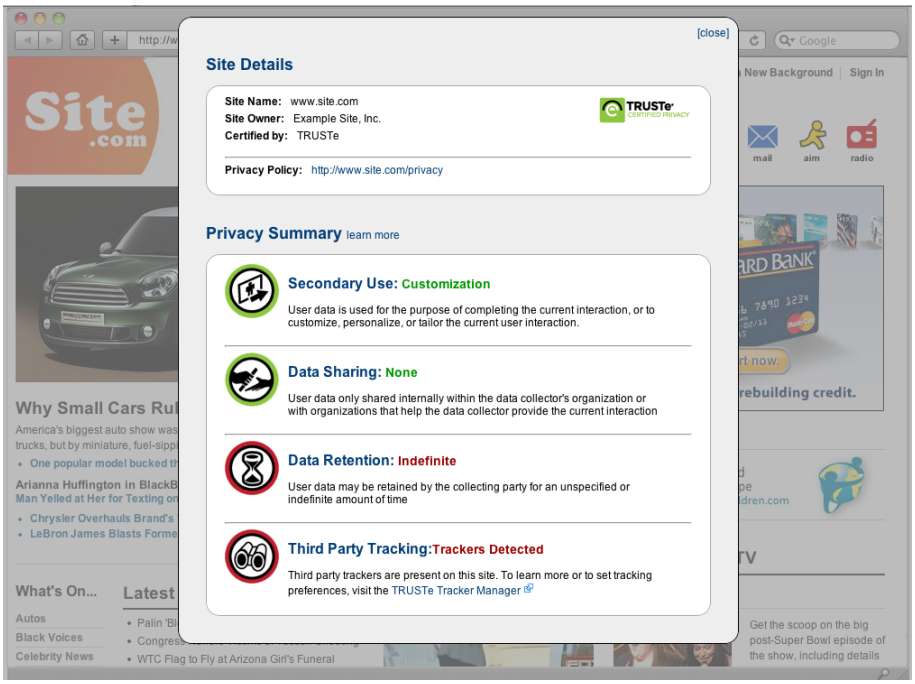
TRUSTe is currently designing an icon-based privacy short notice for simplifying and summarizing consumer-facing privacy statements in a browser-based client. While we intend for this notice to be a consumer-facing TRUSTe presentation layer, we have also designed it so that it could also become an open-source standard for inclusion by browser manufacturers available for certification by other third-party privacy authorities.

In designing this icon-based short notice, TRUSTe is looking at other short notice designs, including the standards for short notice design proposed by Alissa Cooper of CDT and Aza Raskin of Mozilla.[8] Based on our research, the current draft of our icon-based short notice (displayed in Figure 1 below), identifies three types of categories: data use, data sharing, and data retention (focused on how data is used, not what data is collected). We have done some limited user testing around this design and have found that for the most part, users understand the purpose of a short-notice in facilitating online privacy. Our research also shows that users don't necessarily have a

[8] See Travis Pinnick, TRUSTe Blog: Privacy Short Notice Design, February 17, 2011, available at: http://www.truste.com/blog/?p=1253

preconceived notion of what a short notice should look like (icons, categories, colors), and may look to a trusted authority – like TRUSTe – to identify this for them.

Figure 2. TRUSTe's Possible Revised Short-Notice Design



TRUSTe has also been working on developing a short notice format for mobile devices. One of the major challenges here was to provide a comprehensive privacy notice on the small screen. To address this challenge, our short notice format uses a mix of icons and text to address key privacy concerns such as the collection and use of geo-location information on a mobile device. We have provided two examples of our mobile short notice format in Figures 3 and 4 below.

Figure 3 – TRUSTe Mobile Short Notice for Location-Based data

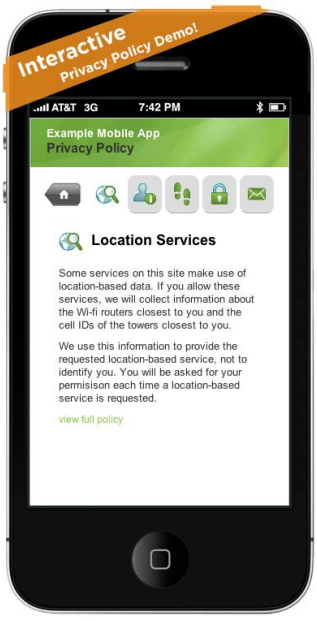
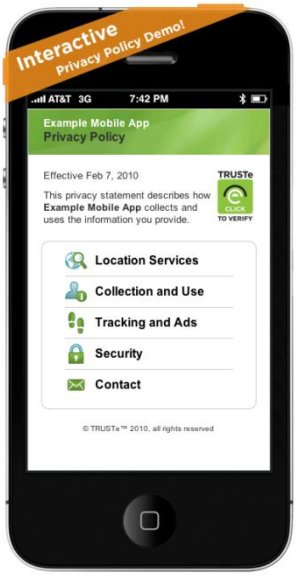


Figure 4 – TRUSTe Mobile Short Notice Format Showing Purpose Specification



TRUSTe has also developed a series of Just-in-Time notices to communicate a new use of personal or sensitive data not previously described to the consumer and any choice options around that use. An example of this type of notice is the Just-in-Time notice presented by the A LOT tool toolbar, which was discussed previously.

TRUSTe also sees a role for browser software to provide notice, as browsers remain the primary mechanism by which consumers access and interact with web products and services. Integrating notice at the browser level can provide a level of technical enforcement to help all sites comply uniformly with a standard that can serve as a foundation for privacy interaction. The SSL padlock model – which has provided "notice" of a website's identity and proof of encryption since the early days of e-commerce – may be illustrative here.

3. Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

TRUSTe supports the use of machine-readable privacy policies that remove the guess work as to what a company's privacy practices are. Combined with other technologies, a machine-readable privacy policy can be more accurate than a text-based privacy policy.

Most companies communicate with consumers about privacy through a text/html-based privacy policy, which may be supplemented with an opt-out/choice service via email or website interfaces. There are many shortcomings and limitations to the current "notice and choice" system, which are well outlined in the FTC Report. As a result, millions of websites have privacy policies, but few consumers are aware that such policies exist (even fewer have actually read and utilized these policies). This is a sub-optimal system.

To address the problem, in most cases, privacy policies need to be augmented with a machine readable, service process-able XML counterpart. This can lead to new applications that could help consumers better understand what is contained in a given site's full policy (including the privacy policies of the site's partners), at the site URL and cookie layers, and for applications that sit on proprietary networks and clients. XML policies can also help sites manage data flows between their site and their partners sites, and provide new foundations for tools that can encode information to provide accountability for that information all the way back to the sourcing consumer.

Several elements are required to build the necessary "trust system" around an xml policy infrastructure, so that a web site's policy can be promoted and read through a browser. These include:

- a method to illustrate the policy in a graphical fashion via iconography or other similar mechanism, to give consumers a tool to compare practices between similar companies, and take into context the nature of the business model and primary purpose for which data is collected and used,

- a method to delineate self-asserted policies vs. policies vetted by a trusted 3rd party which provides accountability services,

- methods to control 3rd parties that are trusted to provide such services,

- methods to access Choice and request for Access mechanisms, and

- methods to provide user feedback and dispute resolution.

A similar set of components can be established for the more general "enterprise" use case of partner management and sharing data across corporate boundaries.
For any trust system to achieve the appropriate level of acceptance and utilization, a combination of industry investment and standards development is necessary to develop the structure, dictionary and usage guidelines of the XML.

TRUSTe's view is that a machine-readable system is relevant now more than ever. Impending requirements from legislative and regulatory bodies, increased consumer awareness around behavioral advertising and social networks, and the advent of more products and services leveraging 3rd parties and privacy sensitive technologies, all lead to a perfect opportunity to address this collaboratively. In addition, there are some lessons learned from past efforts in various different communities that can help shape the effectiveness of such a campaign going forward.

4. Should companies be able to charge a reasonable cost for certain types of access?

TRUSTe requires that sealholders provide consumers a way to update or correct inaccuracies about their personal data free of charge. If however, a consumer's Access request involves an abnormal expenditure of internal resources, then the company should be allowed to charge a reasonable fee. The company should fulfill all commercially reasonable requests for which the consumer is willing to pay.

5. Should companies inform consumers of the identity of those with whom the company has shared data bout the consumer, as well as the source of that data?

Under California's "Shine the Light Law" ("SB 27"),[9] companies must provide a mechanism to allow consumers to opt-out of having their personal information shared with third parties other than Service Providers. If the company does not already provide such a mechanism, then it must provide a way for consumers to request a list of third parties with whom the company has shared the consumer's PII. Allowing consumers to request this list of third parties from a company puts a lot of responsibility on the individual consumer, and is neither effective nor helpful. It also imposes a regulatory burden on the company, who must incur the costs of tracking such requests. Consequently, most companies doing business in California tend to opt for the safe harbor of providing an opt-out mechanism, rather than maintaining a list for anticipated consumer requests.

As discussed earlier, under our updated privacy program requirements, TRUSTe sealholders are required to provide a Just-in-Time notice, along with an opt-out mechanism, if the client shares PII with third parties for unexpected purposes. In a recent survey, TRUSTe found that 95% of the surveyed sites provided heightened notice at the point of PII collection, further strengthening the argument that providing an effective choice mechanism helps companies build consumer trust while also managing the costs of doing business.

6. Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Yes, consumers should receive notice if data about them is used to deny benefits. Credit card companies and other providers of credit are already required to do this under the Fair Credit Reporting Act, which is enforced by the FTC.[10] Typically the notice is sent via postal mail.

[9] SB 27, also known as California's Shine the Light law, was passed in 2003. Full text available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

[10] Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

7. What types of changes do companies make to their policies and practices and what types of changes do they regard as material?

TRUSTe's program requirements address how a company should notify users about the changes to a company's policies and practices that constitute a "material change" in that company's privacy obligations. Under TRUSTe's privacy seal program requirements, a material change occurs when a site reduces privacy protections; this includes changes regarding notice, collection, use, and disclosure of first and/or third party personal information.

8. What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

TRUSTe believes that informed consent and transparency is very important to prospective data handling practices, particularly involving a material change to a company's privacy policy. When a TRUSTe sealholder chooses to make such a change, TRUSTe requires that the company first informs us of these changes. We then work with the sealholder to craft mechanisms for providing notice to users of the material change. TRUSTe thinks that it is imperative that a user has the choice to no longer use a site before a material change takes place. We require our sealholders to provide notice of material changes either via an email or by a notice on their web site, prior to the change becoming effective. TRUSTe believes notice via email or on a website provides the types of transparency about privacy practice changes that provide consumers the information needed to make informed decisions.

9. How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

TRUSTe believes in the importance of consumer education to help consumers make informed decisions about the privacy choices available to them. Consumer education is also important to help us resolve consumer privacy concerns. We think consumer education should be provided appropriate to context e.g. detailed documentation housed in a company's "Help" page, vs. smaller notices for consumers accessing the information on a mobile device. We also think it's important to educate consumers in a manner that respects the consumer's technical understanding of the issue, language barriers, etc.

To educate ourselves about consumers' privacy concerns, TRUSTe reviews disclosures to consumers as part of our standard certification process; we also carefully review reports filed by consumers about our sealholders under our dispute resolution program. Approximately 12% of consumer inquiries TRUSTe receives under our dispute resolution program are resolved through consumer education efforts. Incidentally, the most popular category of questions revolves around how consumers access self-help privacy controls for a particular company's web site. Through our dispute resolution process, TRUSTe regularly directs consumers to other useful sources of information,

such as the FTC's pages on identity fraud, or sources that provide helpful advice on the basics e.g. the need to clear one's web browser cache.

In 2010, approximately 2% of the consumer reports filed resulted in site changes by our sealholders. The most common situations involving such site changes by sealholders are Negative Option Marketing and Contact Import mechanisms that send invites on behalf of the user. As a result, TRUSTe has noticed that fewer consumers filed complaints in 2010. We attribute this reduction in complaints to the improvements by our sealholders in offering privacy choices and controls.

CONCLUSION

TRUSTe appreciates the opportunity to provide its perspective on the important online privacy issues identified in the FTC Report. We believe that the FTC Report is a thoughtful analysis that recognizes the importance of choice and transparency to an online privacy framework.

Overall, TRUSTe supports the scope of the framework, as defined in the FTC Report, as well as the identification of privacy by design, simplified choice and greater transparency as the building blocks of that framework. We would encourage the FTC to craft a framework that is flexible enough to recognize newer, innovative mechanisms for choice and transparency – such as alternative notice forms and machine readable privacy policies. Finally, we would recommend that the FTC recognize Accountability, Access and Accuracy within the substantive privacy protections of the framework.

We look forward to working more with the FTC and with our client companies on operationalizing the relevant portions of the proposed framework into business practice. We thank the Commission and its staff for their review of TRUSTe's regulatory response to the FTC Report. Please do not hesitate to contact me with questions at (415) 520-3400.

Sincerely,

Fran Maier
President