Fran Maier
President
fran@truste.com

January 28, 2010

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

Via: Electronic filing: privacynoi2010@ntia.doc.gov

Re: Docket No. 101214614–0614–01 – TRUSTe's comments in response to the Department of Commerce's Green Paper - *Commercial Data Privacy & Innovation in the Internet Economy: A Dynamic Policy Framework*

TRUSTe supports efforts by the Department of Commerce ("Department") to address the current and important issue of commercial data privacy and is happy to provide responses to the questions posed by the Department in the above-referenced Green Paper.

Overall, TRUSTe agrees with the Department's Internet Policy Task Force on the need to update the existing policy framework to address commercial data privacy issues in the United States. We would emphasize three additional points:

- To work successfully, a domestic policy framework would need to be sufficiently dynamic to manage the needs of all the stakeholders in our diverse, commercial data ecosystem. This means that the framework should not be limited in terms of implementation. It would also need to recognize existing policy frameworks that have been established to deal with specific sectors: financial data, personal health information, etc. The existing frameworks operate with a multi-tiered approach to implementation, evaluation, and accountability. Since each process within the framework will have different motivations and different operational challenges, the roles associated with development, implementation, and enforcement of the policy infrastructure should be flexible, interoperable, and scalable.

- TRUSTe believes that any regulation of commercial data must be executed in a manner that maintains incentives for companies to innovate, while also preserving consumer privacy. Given the dynamism of the commercial data ecosystem, TRUSTe strongly supports working closely with industry to identify and develop solutions to online privacy challenges. On that note, TRUSTe commends the Department's outreach to industry in the research and drafting of this Green Paper.

- TRUSTe's recommendations are based on our experiences working with many of recognizable players in the online ecosystem. Today TRUSTe certifies the online privacy practices of over 4,000 web properties across a variety of platforms and services, including email and advertising platforms, websites, software downloads, and mobile applications.[1] Our diverse client base includes companies of all sizes and industries, from small e-commerce websites to major pharmaceutical companies, as well as top online brands like Apple, Facebook, and Microsoft. One aspect of TRUSTe privacy certification is that companies must agree to ongoing participation in our Watchdog Dispute Resolution Program, which allows consumers to file privacy complaints against our

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

licensees. TRUSTe works hand in hand with the complainant and our client to resolve the issue, and in 2010 we processed over 7,500 such complaints.

Working closely with these clients, TRUSTe has observed many of the changes in the online landscape that are highlighted in the Department's Green Paper. In fact, we are just completing a full revision of our privacy seal program requirements, and plan to release these 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 track the proposed framework outlined in the Department's Green Paper.

Included below are TRUSTe's responses to specific questions listed in Appendix A of the Department's Green Paper:

1. The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

TRUSTe supports a review and reevaluation of the current FIPPs. The current FIPPs were established in the 1970s – before the advent of the commercial Internet and web technologies, at a time when "Social Networks" and "Data Brokers" did not exist. Advances in both technology as well as business models point to a clear need to update our existing framework with a more relevant set of FIPPs.

a. Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?

While TRUSTe supports adoption of a comprehensive set of FIPPs, it may not be necessary to address implementation of such principles through legislation. We view privacy as inherently contextual; disclosure obligations will differ depending on the context of the interaction. Privacy is also subjective, which means that the standard for what constitutes an acceptable disclosure obligation will change depending on social attitudes and mores. This means that a commercial data privacy framework must be sufficiently flexible to stay relevant.

We note that the regulatory frameworks currently in place in the US reflect this inherently contextual nature of privacy e.g. FCRA/FACTA (information used in "consumer reports"), Gramm-Leach-Bliley (information sharing between financial institutions and affiliates), HIPAA (transactions involving protected health information by "covered entities"). A comprehensive data privacy framework will need to integrate these existing regulatory structures; therefore TRUSTe recommends enactment of additional legislation, if needed, only where there are gaps in the current regulatory framework that do not address the updated FIPPs. Furthermore, TRUSTe views the FTC's authority under §5 of the FTC Act as another means by which current privacy laws can be enforced.

b. How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?

We believe that enforcement is the bedrock of any framework for commercial data privacy. However, ease of access and timeliness of response are what will make enforceability components of a policy framework successful. Limiting the enforcement mechanism to the courts or a regulatory body only adds administrative pressure onto the framework, and may not resolve the end user/consumer's issues.

Furthermore, we see an important role for non-governmental entities that work with government regulators to ensure successful enforcement of a commercial data policy

framework. In particular, these entities can assist in decreasing barriers to use and speeding resolution of complaints – two considerations in any enforcement structure. A framework of this type is already seen in the alternative dispute resolution arena. While TRUSTe does not advocate the removal of formal, legal proceedings as an enforcement mechanism, we do support the need to include enforcement alternatives – such as ADR providers, auditors, Trustmark operators and Regulatory Safe Harbor providers - to ensure the scalability and flexibility that the framework will require to be successful.

c. As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?

TRUSTe recommends a results-oriented approach to implementation of baseline commercial data privacy protections. In our view, specific regulatory structures that implicate technology often suffer from two important defects: 1) lack of technical expertise in drafting statutory/regulator language, and 2) near-immediate obsolescence. Specific technological requirements are best left up to standards-setting bodies. Further, to avoid becoming obsolete, regulation should be crafted to avoid the "end run" problem often seen in new technologies or business models around detailed regulations. Due to the complex, multi-layered, contextual nature of commercial data privacy, regulation should only be recommended where its potential impact has been carefully considered.

For a good example of how this could work, TRUSTe would point to the Gramm-Leach-Bliley framework of a) overarching legislation, b) effect-based regulation, and c) standards-body audit foundations demonstrating accountability to the framework.

d. Should baseline commercial data privacy legislation include a private right of action?

Any baseline commercial data privacy framework needs a mechanism that provides the data subject/consumer with a remedy in the event that a breach of the framework occurs. How the mechanism is structured will depend on the contextual risk the data subject takes in the transaction with a commercial actor. As with credit cards, a mere limitation of liability for fraud may be sufficient to engender trust, and remove barriers to growth. However, with higher levels of risk to the consumer, or more tangential the harm, other methods of redress may be necessary.

2. To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority.

Most privacy statements today do not provide the level of transparency needed for consumers to make informed privacy choices. TRUSTe strongly supports enhancing transparency. We believe that 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 consumers have over the use of that data.

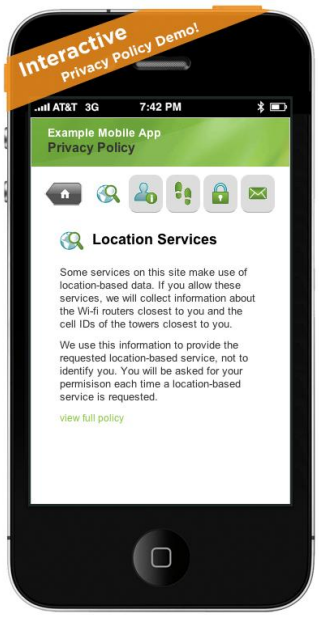
TRUSTe also supports the high priority given by the Department to Accountability, which we view as an important component to an effective privacy framework. We note that Accountability is a cornerstone of many global privacy frameworks including APEC, the EU Privacy Directive, OECD, and PIPEDA. We believe in two types of Accountability: Accountability to the data subject, as well as Accountability within an organization i.e., the mechanism that verifies whether a company is complying with data controls and policies. TRUSTe also believes that there is a need to enforce Accountability outside of a corporate process or judicial system.

2a. What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

Since 1997, TRUSTe has worked with businesses to build consumer trust through online privacy compliance efforts. This experience has given us a unique perspective on the existing challenges around promoting transparency. We see an important role for the private sector to define and implement innovative options around informed choices – which is why we think it's very important that government work closely with industry to define and promote transparency approaches.

For instance, we have worked closely with our seal holders to develop "Short Notices" that work together with a company's comprehensive privacy notice and provide consumers with a snapshot of the company's practices. Short Notices effectively protect consumer privacy in a way that is relevant to the transaction e.g. the collection and use of geo-location information on a mobile device. Our short notice format uses a mix of icons and text to address key privacy concerns - an approach that we have found to be particularly effective. We are currently working towards Short Notice adoption by most TRUSTe seal holders by December 2011.

Fig. 1 – TRUSTe Mobile Short Notice for Location-Based data



Another innovative approach developed by TRUSTe and other companies are “Just in Time” Notices that communicate a new use of personal or sensitive data not previously described to the consumer and any choice options around that use. Our revised privacy seal program requirements expand the definition of “Privacy Statement” to include Short Notices, Just in Time Notices and other alternative notification mechanisms.

Fig. 2 – Apple’s Just in Time Notice for iPhone

In addition, TRUSTe supports the role of browser software to provide notice, as browsers remain the primary mechanism by which consumer’s access and interact with web products and services.

These are a just a few examples of innovative approaches being developed by TRUSTe and many of our private sector clients to promote informed choice and transparency.

2b. What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization’s data collection, use, and disclosure practices?

TRUSTe believes that companies who want to succeed in today’s information-driven markets have strong incentives to encourage the development and adoption of practical mechanisms to protect consumer privacy. Increasingly, consumers are aware of their online data footprint, making privacy an important consideration in deciding whether to use a company’s online services. We've measured firsthand the positive impact strong privacy practices can have on business. Numerous companies have A/B tested TRUSTe's distinctive green privacy seal on their online properties and they consistently find that the seal increases consumer engagement and business. Budshop.com, the official online store for Anheuser- Busch, tested the TRUSTe privacy seal and found that it increased revenue per customer visit by 13%.[2] Debnroo.com, an online retailer,

[2] TRUSTe SureSource Case Study: budshop.com, available at: http://www.truste.com/pdf/SureSource_Case_Study.pdf

specializing in home, garden, and pet products, found that displaying the TRUSTe privacy seal produced a 29% increase in sales.[3]

2c. What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

TRUSTe recognizes the importance of integrating privacy protections into a product's development life cycle. We know that many companies use Privacy Impact Assessments or "PIAs" to help identify privacy issues during product development. In our view, PIAs help companies identify and manage risk after the fact. This is an unworkable approach - particularly with the shorter development cycles seen in today's web technologies. 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. Assessing privacy beforehand is also the approach that better matches the agility of today's technology development life cycles.

2d. What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?

See our answer to 2 c. above. Generally, we do not see PIAs as a comprehensive way to help companies identify commercial data privacy issues.

2e. Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

TRUSTe supports the use of machine-readable formats for all types of privacy policies. We believe that they remove the guess work as to what a company's privacy practices are. Combined with other technologies, a machine-readable privacy policy can actually be more accurate than a text-based privacy policy. We've also observed that machine-readable formats can be more reliable than PIAs in identifying and evaluating lapses in privacy notices.

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

Impending requirements from legislative and regulatory bodies, increased consumer awareness around behavioral advertising and social networks, and the advent of more privacy sensitive technologies, make the issue of machine-readable formats relevant now more than ever. We think this is a perfect time for the Department to start addressing the issue collaboratively – in consultation with other stakeholders and global regulators – and would be happy to assist with that discussion.

[3] Increasing Retail Conversions – TRUSTe seal on debnroo.com, available at: http://www.truste.com/pdf/Debnroo_Case_Study.pdf

2g. What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?

Transparency – including the options and mechanisms for choice - 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, however, short notices can be very effective in delivering high level information in conjunction with the traditional privacy policy. 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.

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 use of icons and other visual cues, 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.

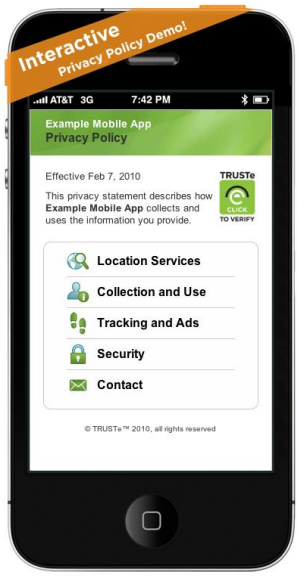
2i. Are purpose specifications a necessary or important method for protecting commercial privacy?

TRUSTe believes that purpose specifications are an important and necessary component to any privacy framework involving commercial privacy. Purpose specifications provide consumers the information they need to make informed decisions about whether to use a particular product or service. We also believe that purpose specifications should provide details of the data's intended use and be offered in a timely manner. In crafting our privacy seal program requirements, TRUSTe was guided by the Purpose Specification Principle of the 1981 OECD Guidelines – which specifically requires that purpose specification occur at the same time or before data is collected.

2k. Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?

Already, we are seeing much innovation around purpose specifications and use limitation mechanisms, particularly on the mobile web. TRUSTe's own Mobile Privacy Requirements utilize a TRUSTe-hosted Short Notice format, which provides enhanced notice outside of the Privacy Statement, about the types of data being collected on the consumer's mobile device. The notice also provides other details about the company's data sharing practices, the consumer's ability to exercise access and notice, whether any tracking technologies are used, which security measures are in place, and how to contact the company. In this way, consumers are presented with information – even on a small screen – to make informed decisions.

Fig. 3 – TRUSTe Mobile Short Notice Format Showing Purpose Specification



This approach also recognizes that mobile is a different platform from the desktop. Consumers may not want the same type of data collected on their mobile device, as they do on their desktop computer e.g. geo-location data that may be considered sensitive.

2l. What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

When it comes to purpose specifications, TRUSTe believes that companies should give consumers enough information to make informed choices. Companies that don't do this, risk losing consumer trust which will ultimately hurt their business. We believe that this is the strongest incentive for companies to state clear, specific purposes when using consumers' personal information.

2m. How should purpose specifications be implemented and enforced?
See our answer to 2.k. above. We think that much of the innovation and implementation should come from industry – as they are closer to the product - but that government regulators should guide those efforts with baseline principles e.g. FTC's Behavioral Advertising Guidelines which prompted the Self Regulatory Guidelines for Behavioral Advertising by the advertising industry (IAB, DMA, AAAA,NAI, etc.).

2n. How can purpose specifications and use limitations be changed to meet changing circumstances?

TRUSTe supports the continued role of industry in defining purpose specifications and use limitations based on the unique needs of a company's business model.

3.b. How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

TRUSTe supports discussion of "Do Not Track" as one of many tools that can be employed within a self-regulatory framework. TRUSTe believes however, that online advertising companies can and will find ways to work around technologies like " Do Not

Track", unless these technologies go hand in hand with self-regulatory frameworks that bring monitoring, verification and accountability to the table. We see an important role for third-party accountability agents, like ourselves, to work with companies and consumers and ensure that transparency, accountability and choice exist in the online advertising ecosystem.

3d. How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

TRUSTe believes that the Department's PPO should work closely with the leadership of the National Association of Attorneys General, including the current President and Chair of NAAG's Consumer Committee, on enforcement of the commercial data privacy framework.

5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

TRUSTe supports the continued role of the FTC as the lead consumer privacy enforcement agency in the United States.

*5b. What should be the scope of FTC rulemaking authority**?***

TRUSTe believes that the FTC should have rulemaking authority over any activity that involves possession and use of consumer data, because all entities that possess and use consumer data about an individual have the opportunity to create harm to that individual. We believe this thinking is in line with the expansive interpretation of the term "consumer" under §5 of the FTC Act. By defining the rulemaking authority so broadly, the Commission should be careful to consider Context when determining the privacy impact of a particular business practice.

5d. Should non-governmental entities supplement FTC enforcement of voluntary codes?

TRUSTe believes private entities should supplement FTC enforcement of voluntary codes. Trusted private entities help enforce transparency by certifying the accuracy of posted privacy policies. These trusted third parties already serve an important role in at least two other successful compliance schemes - PCI (payment card) data compliance and California's system for issuing SSL certificates.

Private entities can serve as enforcement alternatives by providing voluntary industry programs such as Trustmark providers or regulatory safe harbors. It starts with the creation of a co-regulatory framework where private entities must be approved as to meeting certain standards e.g. robust code of conduct, monitoring of program members, dispute resolution and periodic re-certification. This multi-layered co-regulatory approach will enable enforcement alternatives to mitigate any perceived conflict of interest around enforcing a set of standards on its members. Global frameworks such as APEC have recognized and are creating a multi-layered approach for using government approved Trustmarks to supplement enforcement, which is a must in any successful accountability system.

5e. At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.

If there is a law containing a safe harbor provision that requires rulemaking, the FTC should approve any code(s) of conduct. Otherwise, associations should not be restrained from creating their own voluntary codes of conduct. Requiring prior review for voluntary codes of conduct would inhibit the development of such codes.

5f. What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?

If a company publicly attests through a Privacy Policy, Terms of Service, or some other means, that they are following a code of conduct but then fail to do so, they will be subject to an enforcement action by the FTC for deceptive business practices. There are no additional steps or conditions required.

9. Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

Since the nature of eCommerce is inherently trans-jurisdictional, there are a number of Constitutional considerations around the regulation of ecommerce by individual states. When States do regulate, they must be careful to not run afoul of both the active and dormant commerce clause, which prohibit States from discriminating against interstate commerce.

TRUSTe believes that a policy framework around commercial data must be developed and mandated at the federal level because where individual states impose obligations on out-of-state businesses, with no nexus to that business, the constitutional nature of the obligation becomes suspect, adding to uncertainty.

9a. Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

TRUSTe believes that the FIPPs structure is appropriately broad to create a foundation for commercial data privacy policy and should be mandated for national application. State level evaluation and regulation of emerging business models will inject uncertainty into the process and thus chill innovation. Where the framework speaks to privacy-specific harms, it should be national in scope. To do otherwise will encourage "forum shopping" in those states that might provide less protection to data subjects/consumers. Such inconsistency will also operate to slow trust in web commerce.

9b. How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?

Current privacy bills and consumer protection laws effectively balance state needs with federal preemption. Where a FIPP-based framework relies on legislative or regulatory instruments to enforce the framework, this mechanism of broad federal preemption with state elevation of some requirements should work well. However, there may be uncertainty when State laws provide increased protections under the Constitution's commerce clause.

9c. To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation? Support?

As was noted earlier, a robust FIPPs framework will include layers of enforcement tools. Joint enforcement by the FTC and the State Attorneys General have been shown to work well in this type of environment. Consequently, a FIPPs-based framework should be reviewed and implemented as appropriate.

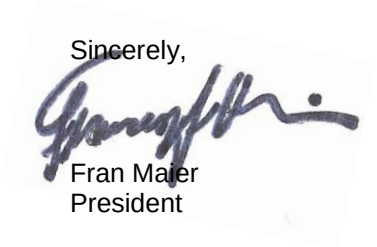
9d. Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

Data protection - as a right - is currently enforced as a "deceptiveness" issue. However, taking data protection into the next century exposes the deficiencies of this approach e.g. this approach would not provide a remedy absent a lack of financial harm to the individual. A robust framework based on the FIPPs resolves the problem by imposing rights and obligations directly onto the commercial actor outside of the "deceptiveness" framework defined under state laws. As a consequence, a nationally-based commercial data privacy framework would not be in direct conflict with state deceptive trade practice statutes, and pre-emption will not be an issue. In the event that data protections contained by the FIPPs framework continue to use "deceptiveness" as a jurisprudential basis, the current framework of authority-sharing between the FTC and the States can be used as a model to allow for the balanced and effective protection of both sets of interests (state & federal).

Data protection - as a right - is currently enforced as a "deceptiveness" issue. However, taking data protection into the next century exposes the deficiencies of this approach e.g. this approach would not provide a remedy absent a lack of financial harm to the individual. A robust framework based on the FIPPs resolves the problem by imposing rights and obligations directly onto the commercial actor outside of the "deceptiveness" framework defined under state laws. As a consequence, a nationally-based commercial data privacy framework would not be in direct conflict with state deceptive trade practice statutes, and pre-emption will not be an issue. In the event that data protections contained by the FIPPs framework continue to use "deceptiveness" as a jurisprudential basis, the current framework of authority-sharing between the FTC and the States can be used as a model to allow for the balanced and effective protection of both sets of interests (state & federal).

We thank you for the opportunity to submit these comments, and look forward to working closely with the Department on these important issues. Please do not hesitate to contact me with questions at (415) 520-3400.

Sincerely,



Fran Maier
President