June 7, 2010

Office of the Secretary;
National Telecommunications and
Information Administration;
International Trade Administration
U.S. Department of Commerce,
1401 Constitution Avenue, NW., Room 4725,
Washington, DC 20230

Re: Department of Commerce Notice of Inquiry
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174–0175–01; RIN 0660–XA12

TRUSTe Comments

On behalf of TRUSTe, I thank you for the opportunity to share our reflections on the Department's core inquiry concerning the nexus between privacy policy and innovation. Our intervention reflects the experience that we have gained in helping more than 5,000 companies over the course of a decade build trust with consumers online through our certification programs and addressing privacy through best practices.

Our experience and research shows that consumers are more comfortable with innovation and new business models on the Internet when their privacy expectations and protection of personal information is considered in the design and rollout of services. Consumers look for signs of trustworthiness of companies they may deal with online, including by looking for trustmarks and third party certification programs. They are more likely to register at websites, complete e-commerce transactions, and engage in internet use for social networking, e-mail, entertainment, or for general information gathering purposes when they see one or more seals that they trust on a website. It should come as no surprise then that 71 percent of consumers said they look for trustmarks before doing business online.[1]

Businesses that are sophisticated and care about demonstrating privacy accountability to consumers look for opportunities to meaningfully differentiate their practices based upon best privacy practices and outward demonstrations to consumers, such as through trustmarks and third party certification programs. They do so because it builds and retains consumer relationships and generates a

[1] "Trust Marks: What's Behind the Label Counts". Yankee Group. 2009. http://us.mcafee.com/en-us/local/docs/LR-51384.pdf

positive return on their investment through higher registrations, transactions, and more accurate data. Smaller and medium-sized businesses (SMBs) need greater opportunities, at affordable prices, to leverage privacy as a part of their brand differentiation and to build consumer traffic online. TRUSTe is innovating to fill that gap in the online market place. We appreciate the positive role of government to encourage forward leaning privacy policy nationally in order to assist all U.S. businesses to be competitive in the global online marketplace.

What is the impact of current privacy laws in the U.S. and around the world on the pace of innovation in the information economy?

Businesses and consumers are confused about varying privacy requirements across global jurisdictions, as well as differences presented with respect to specific business sectors. In many instances, business and consumers do not know or understand what protections are required or avenues of privacy recourse available. The cost of business compliance with such a wide range of legal and regulatory requirements may actually limit consumer choice because of slower innovation of online services caused by reticence. Innovative ideas may be sidetracked simply because businesses cannot interpret a patchwork of privacy laws. By example, crowd source, data such as individual reviews of businesses voluntarily provided by individuals, may be helpful to consumers in determining their own choices around specific stores, goods or online services. However, restrictions on data flows of crowd source data provided in one global jurisdiction from free transfer to another jurisdiction may inhibit such sharing and the accuracy of research and representations of overall consumer experiences and, thus, impact negatively on consumer choice and limit business opportunity. Harmonization of privacy frameworks and policy approaches to privacy online would assist businesses in delivering communications, products and services to consumers and assist with their efforts to be accountable for consumer privacy.

Do current U.S. laws serve consumer interests and fundamental democratic values?

The free flow of information on the Internet is important to fundamental democratic values, as is the protection of individual privacy. With regard to individual privacy, we believe that an improvement for the protection of users globally would be greater access to independent dispute resolution for their privacy concerns and complaints with commercial entities. Mechanisms for promoting more efficient, effective and low cost complaint resolution for consumers through non-governmental programs, regardless of borders, could improve consumer satisfaction, advance public policy for a fair and open online market place and would engender greater trust online. It remains important for consumers to have access to government redress, but those processes are often too time consuming, expensive, and as a result, ineffective for addressing privacy issues where harms can be mitigated by early resolution. Other self-regulatory mechanism that provide monitoring of practices online will also keep businesses accountable to consumers in actual practice.

Specific Areas of the Department's Inquiry:

1. **U.S. Privacy Frameworks Going Forward**

TRUSTe POV: We believe that promoting an understandable roadmap of best practices principles for businesses and signs for consumers on the Internet, short and easily recognizable – through seals, icons, symbols, will prove most helpful on websites and interactive or mobile tools that link users to the internet.

Strong Notice remains essential and we believe that there are new ways to deliver recognizable messages and signs about privacy to busy consumers who may be looking at very small screens on devices and choosing to make an e-commerce or communication decision. Some mechanisms deserving consideration include browser embedded notices, much like SSL padlock icon for e-commerce; new short notice formats for mobile devices and smart phones; Ad unit notices, and movements back to machine readable policies, learning from the P3P experience.

Businesses need incentives and help in ramping up to use short disclosures and seals so that consumers will easily understand them. By example, among other incentives, tax credits to businesses might help spur the uptake of privacy awareness and best practices that can be independently assessed by third parties. The net result could grow and preserve the online market for U.S. innovation around privacy and build consumer confidence in not only in the U.S. but also globally.

We also believe that there remains a place for longer privacy policies that make full representations that consumers can study and rely upon for enforcement of commercial promises.

Separately, consumers are looking for more accessible means of indicating their choices around privacy preferences, both in and outside of the privacy policy, as most visibly indicated in recent reactions to changes in Facebook's privacy controls.

What is the current state of privacy self-regulation? Should there be minimum requirements for self-regulatory programs? If third parties conduct those programs, rather than as a company's own internal operations, what mechanisms should there be for users and civil society to provide input?

TRUSTe POV: TRUSTe has been an independent third party provider of privacy and trust certifications for online services for more than a dozen years. We are supportive of proposals for the enactment of a federal law requiring privacy disclosures online in order to enhance business and consumer awareness of privacy protection. A federal law would extend the impact of certain state laws, like California's, that require privacy disclosures and advance opportunities for consumer choice, and would provide a recognized national standard. Self-

regulatory programs can work in tandem with legislation in this area, strengthening implementation and effectiveness.

TRUSTe, is an independent third party whose privacy certifications are criteria-based, built around solid program requirements that incorporate the fair information practices principles and international privacy principles and best privacy practices. While those requirements evolve with changing business models, new technology approaches and privacy risks online, we believe that self-regulatory programs are best when they are criteria based. As a baseline, they should include thorough certification practices, ongoing monitoring of business practices against their policy statements and self-regulatory program requirements, compliance and enforcement mechanisms, and means for dispute resolution. All stakeholders, including users and civil society are able to provide input into privacy self-regulatory programs when the programs are sufficiently transparent with the ongoing development of requirements and reporting on operations, consumer complaints and effectiveness in responses, and compliance and enforcement activities. Self-regulatory programs are strengthened with this input. Third parties need to publish their program requirements, much like SSL certification authorities publish their Certification Practices Statement. Eventually, it may be possible to establish some technical audit mechanisms, including browser audits of certification authority privacy program requirements, following recognizable standards, similar to the audit model for SSL certification authorities.

Self regulatory programs can support the current notice and choice approach in the U.S., modifications on it, or approved uses of information under a use-based approach that some are currently advocating. TRUSTe believes it will remain essential for consumers to have clear privacy disclosures, easily readable privacy signs (seals and symbols), and consumer opportunities for access to information use by companies and preservation of consumer choice around information use.

We also believe that positive incentives, for example the benefits that organizations enjoy with a credible trustmark (higher registrations, transactions etc.) provide a positive incentive for strong privacy programs.

2. **U.S. State Privacy Laws – Whether the diversity of state privacy laws has a positive, negative, or neutral impact on the privacy rights of Internet users and presents hurdles for businesses**

TRUSTe POV: TRUSTe works with companies across the United States that participate in interstate commerce via the Internet. The patchwork quilt of privacy and information security and data breach laws across the nation is difficult for many of our clients to navigate. It is also difficult to offer a self-regulatory program that addresses compliance with all of the state laws, so instead, best practices and requirements are targeted to federal standards. We believe greater harmonization would certainly provide clarity for businesses. It would better assist good companies that want to fulfill privacy requirements with a clear path to do so in a

consistent manner across state jurisdictions and affording consumers the same treatment.

3. **International Privacy Laws and Regulations – What challenges do businesses face when trying to transfer data across borders? What lessons have been learned from the U.S. – EU Safe Harbor Framework that could be applied in the global context? What mechanisms do organizations use to enable cross-border data transfers?**

TRUSTe POV: Companies are required to honor limitations on cross-border data transfers of personally identifiable information from jurisdictions such as the European Union, and certain non-EU countries with similar restrictions, unless they use legal mechanisms to provide assurances of adequate treatment of the data by the cross-border recipient. This is a complicated process for sophisticated and large global companies and, frankly, we believe not known or understood by small and medium sized companies on the Internet that may also be required to abide by these legal restrictions.

TRUSTe has provided a EU Privacy seal program since 2001 to assist companies in meeting their compliance readiness obligations when they self-certify to the U.S.-EU Safe Harbor Framework with the Department of Commerce. Through our program we provide dispute resolution services, as called for by the Framework. We have learned that nearly every company in our program needed assistance in complying with the Framework's principles, including changes to their processes or consumer disclosures. We also have seen that the Framework is working in terms of consumer knowledge, as the rate of consumer complaints has increased with awareness of the ability to file online complaints and have them resolved.

We believe that the Safe Harbor Framework is a good starting point for other global privacy mechanisms, particularly because it is principle-based and allows for respect for both U.S. and EU legal frameworks and privacy values, with important requirements around notice, choice, and dispute resolution. As additional frameworks are contemplated, we look for them to include workable onward transfer provisions.

TRUSTe is active in ongoing efforts in the Asia Pacific Economic Cooperation forum to advance cross-border cooperation and enforcement of privacy commitments. We support the leadership of the Department in this international effort, including the work that encourages criteria-based self-regulatory programs for qualification as APEC privacy accountability agents. We also support APEC's testing of APEC certification programs that require ongoing monitoring of business practices, have compliance and enforcement mechanisms, a direct means for consumer dispute resolution and encourage transparency on results.

4. **Sectoral Privacy Laws and Federal Guidelines – What can be done to make the current sectoral approach to privacy regulation in the U.S.**

more conducive to business development while ensuring effective privacy practices?

TRUSTe POV: We believe that it is important to acknowledge specialized expertise of regulatory agencies for specific sectors. At the same time, it is important to distinguish between specialized experience in a particular business area requiring specialized regulation, for example financial services, and common, national priorities and best practices for business protection of consumer privacy.

We are concerned about impediments to innovation in both product delivery and privacy protections, in particular in the financial services sector at a time, when consumer certainty and trust need to be bolstered. Recently the financial services regulators came out with a model privacy statement and an online version that financial institutions must use in order to receive safe harbor regulatory compliance treatment. TRUSTe is particularly concerned because the model privacy policy does not allow U.S. financial institutions to use a seal on their privacy policy. Consumers looking for greater confidence in the financial sector are singularly unable to receive a sign that the policy and practices behind the privacy policy have been reviewed and certified by an independent third party, or that they are participating in a program that offers ongoing monitoring of privacy promises, compliance and enforcement, and third party dispute resolution.

Other sectors receive a competitive advantage by being able to engage more dynamically with consumers online by showing seals on their privacy policies, receiving additional returns on investment and consumer loyalty. TRUSTe believes that it is a mistaken government policy that has no statutory underpinnings. It undermines harmonized privacy protection on the Internet by U.S companies. The policy decision by financial regulators inhibits differentiation of financial brands for businesses and consumers based upon privacy, and results as a restraint on trade for self-regulatory programs like TRUSTe that have a decade of experience in building trust online and promoting U.S. business innovation. This is one example of U.S. vulnerability in a global marketplace where sectoral applications of law and policy around privacy are inconsistent. Those inconsistent applications do not send a harmonized message to raise privacy awareness and may disadvantage the competitiveness of businesses that would like to differentiate their brand based upon privacy practices.

As Congress and policy makers consider federal legislation to address privacy, TRUSTe believes that including a safe harbor concept for companies participating in strong, criteria-based self regulatory programs that demonstrate their accountability for consumer privacy should be a priority. We believe that effective privacy self-regulatory programs also should include substantial monitoring and compliance mechanisms, enforcement authority, and dispute resolution and that program requirements and activities advance consumer confidence through their transparency. To be effective, meaningful incentives for business uptake must also be provided.

5. New Privacy Enhancing Technologies and Information Management Processes

TRUSTe POV: The need for privacy enhancing technologies, whether built into products, added on to products and services, or used by a third party to manage and monitor commercial activities, has never been greater. With wider use of online services for communication, e-commerce, entertainment, and educational purposes, the impact on individual privacy also continues to grow. TRUSTe supports and encourages the Department in its efforts to promote innovation to support privacy enhancing technologies and information management processes. We believe it would be most effective through the promotion of research, public and private partnerships, and incentives to businesses to develop privacy enhancing technologies writ large.

Much as we encourage green activities with respect to care of our physical environment, now is the time to encourage the use of technology to build in and support consumer privacy choices and business privacy advancement in the online environment. This is particularly needed to assist small and medium sized businesses, as well as to meet privacy issues raised by new and emerging business models that may introduce wider privacy impacts across platforms. With encouragement, a U.S. privacy model that embraces technological innovation to support consumer privacy can result in an expectation of excellence in privacy practices that global participants can count on when they interact online with U.S. companies of any size.

TRUSTe POV:

6. Small and Medium Sized Businesses – Challenges and Need

TRUSTe POV: Today, the majority of businesses online are small or medium sized businesses. TRUSTe's research indicates that the vast majority of these SMBs are unprepared to address privacy or information security. Specifically, we found that a majority of small and medium-sized business websites do not have a privacy policy[2]. Many are unaware of domestic or international privacy laws that may apply to their businesses in the online or offline contexts. And, as with many large and sophisticated organizations, SMBs require capacity building and education in order to address business responsibilities to consumers on privacy and information, although they may be both short on time, money and staffing to do so.

TRUSTe is addressing the particular needs of SMBs by raising their privacy awareness and offering products and services that are affordable and result in an up-to-date and accurate privacy policy, describing their information practices with respect to consumer information. We have invested in innovations that including an interactive privacy generator geared to SMB business models, up front and periodic site monitoring, and mechanisms to provide dispute resolution. As we

[2] TNS – TRUSTe SMB Privacy Assessment, Dec 08

deliver the privacy policy and through customer contact, including due to monitoring, we look for teaching moment opportunities to further build SME capacity around privacy awareness.

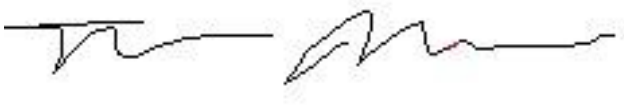
The Department has long included support for SMB training and capacity building. We encourage that continuing role and support through technical assistance. As the Department considers additional ways of building SMB capacity around privacy, it may be helpful for the Department of Commerce and NIST, in particular, to consider the need and utility for a 'PCI'-like standard for SMBs to adopt privacy controls. By example, currently Google Adsense is a good example of a company initiative that requires SMBs advertising through their site to have a privacy policy. But, there is no industry requirement that either requires an accurate statement of privacy practices or that monitors for the existence of policies when requested by company initiatives. There are many avenues for influencing SMB uptake of privacy policies and baseline controls for their online practices, including through ad networks, web hosts, e-commerce sites, and merchant networks. To the extent that consumers have more confidence that SMBs online understand their privacy interests and will be accountable with their data, e-commerce development through U.S. sites could dramatically increase and in a manner that distinguishes U.S. businesses.

7. The Role of Government and DOC

TRUSTe POV: TRUSTe applauds the recent DOC conference on privacy and innovation, as well as the longstanding leadership and commitment of the Department on privacy, particularly with regard to e-commerce and international frameworks between the U.S. and EU and in the APEC forum. We encourage the Department to continue its efforts to advance U.S. competitiveness in the global marketplace by encouraging government and the private sector to work together to demonstrate U.S. leadership broadly in developing and implementing best privacy practices in the online environment.

We encourage the DOC to continue to actively engage with U.S. businesses to monitor privacy and innovation challenges. We believe that the role of government and the DOC is to advance both goals. TRUSTe stands as a ready partner with the Department in continuing working toward that goal.

Sincerely yours,



Fran Maier
President and Executive Chairman