Written Testimony of

CHRIS BABEL

Chief Executive Officer

TRUSTe

before the

House Judiciary Committee, Subcommittee on Intellectual Property,
Competition & the Internet

"New Technologies & Innovations in the Mobile & Online Space
and the Implications for Public Policy"

June 19, 2012

Chairman Goodlatte, Ranking Member Watt, and distinguished members of the subcommittee - my name is Chris Babel, and I am the Chief Executive Officer of TRUSTe, a leading provider of privacy technology and certifications to online companies.

Based in San Francisco, California, TRUSTe offers a suite of privacy solutions to help businesses increase customer trust and engagement across all their online channels - including websites, mobile applications, online advertising and cloud services. Over 5,000 companies including Apple, AT&T, Disney, eBay, HP, Microsoft, Nationwide and Yelp rely on TRUSTe to ensure compliance with evolving and complex privacy requirements and build trust with consumers.

TRUSTe was originally founded as a non-profit industry association in 1997. In 2008, we converted to a for-profit company with venture capital investment. This corporate transformation and infusion of resources has allowed TRUSTe to meet evolving privacy challenges head on in the marketplace. In these past four years we have developed robust technology platforms and rapidly expanded the scope and scale of our privacy offerings and certifications. Our products are cost-effective, scalable, and relevant across business models and practices. Consumers, businesses and regulators worldwide recognize the green TRUSTe Privacy Seal, awarded to our clients upon successful certification, as a symbol of strong privacy practices and trust.

TRUSTe's mission, "Truth in Privacy", embodies our overarching goal of bringing greater Transparency, Choice and Accountability to consumers online. We design all of our products and services around these three core principles:

- Transparency – accurate and comprehensive disclosures through the organization's privacy statements and consumer education initiatives
- Choice – mechanisms that allow consumers to proactively set boundaries around the collection and use of their personal information
- Accountability – the ability for consumers to resolve privacy concerns either with the organization directly or through TRUSTe

I would like to highlight three topics in my remarks before the subcommittee today: 1) the consumer's perspective on privacy; 2) new privacy challenges that exist today, and the technologies that TRUSTe and others have developed to address these challenges; and 3) why we think that self-regulation has been successful in protecting consumers online.

The Consumer Perspective

We believe it is critically important to understand consumer privacy perceptions and attitudes when designing privacy frameworks. Toward this end, we have contracted top research firms over the past three years to conduct numerous national surveys to gauge

consumer privacy attitudes and opinions. Key findings that we would like to share with the committee include:

- 90 percent of U.S. adults worry about their privacy online.[1]
- 85 percent of consumers want to be able to opt-in or out of targeted mobile ads.[2]
- Consumer favorability towards targeted advertising doubles if they are assured that personally identifiable information is not used in the process.[3]
- 74 percent of consumers believe it's "very important" or "extremely important" to understand what personal information a mobile app collects.[4]
- 1 in 3 consumers feel that they don't have a choice when it comes to apps collecting their location data.[5]
- Financial information, direct contact information, health information, and current location are the most sensitive categories of information for consumers when it comes to sharing that data with advertisers.[6]

While many of these responses highlight the fact that there is still considerable work to be done, one additional point worth highlighting is that

- 59% of consumers generally trust that most websites protect their privacy online.[7]

What does all of this mean? The research shows that consumers are becoming more engaged in privacy decisions and more likely to take control of when and how their data is collected and used.   It also highlights the investments many companies have made to follow privacy best practices and build consumer trust online.

The Privacy Explosion: New Privacy Challenges and Technologies to Address Them

There is no end in sight to the tremendous growth of privacy services. In 2011 TRUSTe completed online privacy certifications for nearly 4,000 companies and successfully resolved over 8,600 consumer complaints (not all were privacy related) through a dispute resolution service we offer free to consumers on behalf of our clients. A copy of our 2011 Transparency Report is provided as an attachment to this testimony and provides further detail on our technology platforms, certification processes and dispute

---

[1] http://truste.com/consumer-privacy-index-Q1-2012/

[2] http://truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/

[3] http://truste.com/ad-privacy/

[4] Ibid

[5] Ibid

[6] Ibid

[7] http://www.truste.com/consumer-privacy-index-Q1-2012/

resolution mechanism. Today, I would rather talk about the privacy challenges that lie ahead and the technologies being developed to address them.

The rollout of new technologies and platforms continues at a rapid pace and companies like TRUSTe that offer privacy solutions must move as quickly. The industry shift to mobile devices and the cloud, the growth of online behavioral advertising, and changing global standards have created new privacy challenges, particularly given the underlying reality that data is easier to collect, cheaper to store and faster to analyze (often referred to as "Big Data") than ever before. Let me describe each of these challenges more fully.

<u>Mobile & Wireless Devices</u>

Mobile devices – especially smartphones – present unique privacy challenges because they are carried by many consumers at all times and are in a state of perpetual data collection. There are also challenges around providing consumers with adequate notice and consent mechanisms on a very small screen. We have attempted to meet these challenges in the mobile space in several ways:

- In 2010 TRUSTe launched the industry's first mobile app privacy certification program, leveraging technology to verify app data collection and requiring extra privacy protections around sensitive data collections like user location data. That same year we also introduced an innovative privacy policy format for mobile devices that makes privacy policies readable and user-friendly on mobile devices (see Figures 1 & 2 on next page).

- In 2011 TRUSTe released a free online privacy policy generator leveraging this mobile format, allowing app developers nationwide to create policies for their apps and mobile websites.

- In 2012 we partnered with the Application Developers Alliance to educate mobile developers on important privacy issues as part of a countrywide educational roadshow. This year, we also launched TRUSTed Mobile Ads, a pioneering technology platform that notifies consumers of advertising tracking on their mobile devices and enables them to opt-out if they desire.

Figure 1 –
TRUSTe Mobile Privacy Policy

Figure 2 –
Tracking & Ads Disclosure Section

Cloud

Software is increasingly imbedded in all aspects of daily life. With the increases in bandwidth and connectivity over the past decade, software has transitioned from being managed on premise to being managed in the cloud, often times at locations that are unknown to the end customer. These cloud services are used for everything from backing up consumers' computer files to housing the corporate records and financial statements of some of the largest companies in the world.

To address the privacy challenges of cloud services, TRUSTe added new certification programs to help consumer or business customers understand the data collection, storage and use practices of these cloud service providers.

Online Behavioral Advertising

The sheer scope and complexity of online tracking and advertising given the rise of "Big Data" have created daunting privacy challenges. Consumers have historically been under educated regarding targeted advertising and did not have meaningful control over their data. Industry has banded together to form an organization called the Digital

Advertising Alliance (DAA). This effort, spearheaded by the American Association of Advertising Agencies, the American Advertising Federation, the Association of National Advertisers, the Better Business Bureau, the Direct Marketing Association and the Interactive Advertising Bureau has developed www.aboutads.info to educate consumers and give them control over targeted ads.

TRUSTe is a service provider for this industry effort. Our TRUSTed Ads program is a technology platform that provides consumers with privacy notice and opt-out choice for targeted advertising on webpages and display ads where tracking occurs. Today we are the largest independent provider of compliance technology for the DAA program.

Changing Global Standards

Privacy has become a global issue and other countries have adopted different frameworks and regulations. For instance, TRUSTe has kept a close eye on data protection developments in the EU. As an EU Safe Harbor Provider since 2001, we have helped many clients comply with the EU's unique data protection requirements around data transfers. Earlier this year, we began delivering privacy solutions to provide users choice and notice under the EU's new "Cookie Laws" which regulate online tracking and targeted advertising.

These solutions include our EU Cookie Audit, a powerful auditing technology that can detect and report on all first and third-party tracking mechanisms present on a website. Our clients operating in the EU have used this auditing technology to gain key insight into the scope of data collection on their properties and to prepare for compliance with EU privacy laws. These clients then use our TRUSTed Consent Manager (see Figure 3) on their sites to allow consumers to express or withdraw their consent to be tracked. The Consent Manager can be implemented based on the specific requirements of each EU Member State's Cookie Law.

Figure 3 – TRUSTed EU Consent Manager
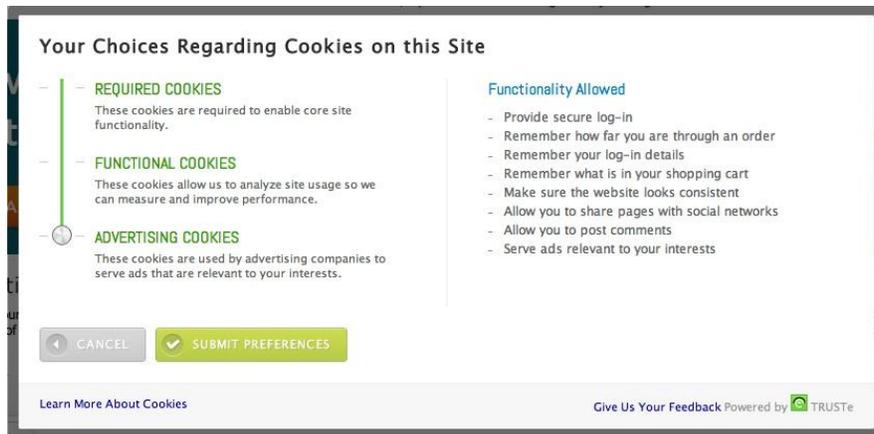
Self Regulation Works

TRUSTe has helped thousands of companies self-regulate their online privacy practices for 15 years and this experience has reinforced our belief that self-regulation is a critical component to any privacy framework. We think that there are at least 3 reasons why self regulation works when it comes to online privacy and data protection:

Self-Regulation Facilitates Global Best Practices. Self-regulatory programs like those offered by TRUSTe can integrate national and international privacy frameworks into a unified program that allows companies to satisfy regulatory requirements and best practices from around the globe. The advantages of making a set of unified changes, instead of continually re-adjusting them for each market and jurisdiction cannot be overstated and create a powerful incentive for companies to self-regulate to higher standards than might be required in any one jurisdiction.

Self-Regulation Can Evolve With Technology – Online privacy frameworks must be dynamic, like the technology they regulate. At TRUSTe, we are constantly adding and updating our program requirements to keep pace with the fascinating and rapidly changing technologies we are seeing in the marketplace. We remain committed to recommending privacy standards that evolve with technology and that are appropriate – not just to the context, but also the privacy expectations of the transaction. This contextual approach helps us adapt our frameworks quickly in response to emerging online and mobile services.

Self-Regulation Can Provide Strong Incentives for Compliance – Self-regulation can encourage compliance by industry through participation incentives. Two important incentives include:

- **Safe harbors** to help foster the growth and promotion of best practices, which in turn are critical to the overall success of a self-regulatory framework.

- **Due Process** to preserve incentives for companies to certify and self-regulate their privacy practices within voluntary frameworks. Under TRUSTe's certification process, due process includes appropriate confidentiality and adequate procedural safeguards, and the opportunity to cure a mistake.

Conclusion - Looking Ahead

As the leading provider of privacy technology and certifications to online companies TRUSTe has had unique insights into the technology changes driving the online ecosystem and their privacy impacts. Looking ahead we see three major trends that will impact future privacy frameworks:

- **The Engaged Consumer** – It is clear that consumers are becoming ever more aware of how their personal data is collected and used online. Mainstream press coverage on privacy has increased significantly in the past few years and consumers have become better informed and proactive about protecting their privacy across devices and platforms. The availability of usable privacy tools and meaningful privacy disclosures will become even more important as this trend continues.

- **Big Data** – Today's companies are racing ahead to harness the aggregate power of vast databases of personal data.[8] Personal data is a critical asset for businesses and leveraging that data can yield tangible benefits for both business and consumers. For example, by leveraging its clinical and cost data, Kaiser Permanente was able to attribute 27,000 deaths to Vioxx and pull the drug off the market. [9] As companies accelerate their use of "Big Data" we see technology playing a much larger role in protecting user privacy in online ecosystems.

- **The Rise Towards Accountability** - Consumers, industry groups and international bodies are all calling for frameworks that hold industry participants accountable to the promises they make to consumers and the standards they voluntarily adopt – regardless of the platform or device that is being used.

For these reasons, TRUSTe believes in self-regulation as a critical component in addressing online privacy challenges. Self-regulation provides a flexible privacy protection framework that can quickly adapt to rapidly evolving technologies. Industry has made great progress on self-regulating their privacy practices, and though there is still much work to be done, we are confident that the goal of protecting consumers - while continuing to innovate – will be achieved.

Thank you for the opportunity to testify today. I look forward to your questions.

---

[8] Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stan. L. Re. Online 63 (2012).
[9] Id at 64.