CompTIA

April 2, 2012

Honorable Larry Strickland, Assistant Secretary

National Telecommunications and Information Administration

1401 Constitution Ave, NW

Washington, DC 20230

Dear Assistant Secretary Larry Strickland,

The Computing Technology Industry Association ("CompTIA") respectfully submits this response to the National Telecommunications and Information Administration request for comments ("RFC"), dated March 5, 2012.[1]

CompTIA is a non-profit trade association representing the information technology (IT) industry, and represents over 2,000 IT companies and 1,000 business partners. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. These members include computer hardware manufacturers, software developers, technology distributors and IT specialists that help organizations integrate and use technology products and services. CompTIA also develops vendor-neutral certifications, with and for the IT industry, such as: CompTIA A+ Network+, and Security+ certifications. CompTIA is the largest provider of vendor neutral certifications in the United States and there are currently over 1.5 million holders of CompTIA certifications held worldwide.

We appreciate the opportunity to share with you 1) our support for a multi-stakeholder process that is robust and leverages all of the tools of technology to ensure input from small and medium sized IT ("SMB") firms is received; 2) our belief in an updated but self-regulatory model of consumer privacy

[1] Federal Register / Vol. 77, No. 43 / Monday, March 5, 2012 / Notice

from which springs enforceable promises subject to litigation under Section 5 of the Federal Trade Commission Act;[2] and 3) our commitment to industry-led standards and certification.

1. Implementing a Multi-stakeholder Process

I. We Should Leverage Technology to Allow for a More Inclusive Multi-stakeholder Process

Small and medium size (SMB) IT firms and businesses are critical stakeholders to the Internet ecosystem and their input should be included. We note for example, that one of our member companies, viaForensics, is a recognized expert in the field of mobile security and is similarly submitting comments to NTIA on this matter. However, because of limited time and resources the majority of IT SMB's often rely on trade associations like CompTIA, and others to represent their public policy interests. The trade association plays a vital role in making sure that the broad sector is adequately represented and has a voice in public policy discussions. Thus, CompTIA proposes that the comment mechanism for the multi-stakeholder process would benefit greatly from leveraging the latest technology.

There are several social networking and communications platforms that can be used to create a broader engagement of community stakeholders. For example, virtual town hall meetings and crowdsourcing could allow for a much more dynamic exchange on these very important public policy issues. Virtual engagement should weigh equally to in-person meetings. In-person meetings are most productive for "inside the beltway" professionals and not as productive for entrepreneurs focused on building new businesses.

Thus, we encourage NTIA to develop a multistakeholder process that is supported not only by publicly written comments and in-person meetings, but also supported by a more robust online and virtual process of engagement. While several agencies have relied on webcasts to conduct public policy workshops, NTIA should use additional online resources such as twitter, Facebook and Skype to stimulate public engagement. CompTIA and other associations can be the conveners of such efforts,

[2] Federal Trade Commission Act, 15 USC 45.

maximizing the expertise of its membership. For example, an effort to undertake a pooling or a joint campaign of industry social media properties to generate comment and input could prove helpful to the process. In addition, crowdsourcing working groups could be created to tackle specific public policy questions.

CompTIA recognizes that there are many perspectives that may be in conflict with each other and it is therefore challenging to develop consensus for various opinions, recommendations, and lessons learned. The multi-stakeholder process will surely reveal this dissonance. As discussed herein, the decision making process for establishing consensus must be flexible. To the extent enforceable codes of conduct are adopted, they should serve as guideposts that are continually revisited on a periodic basis. Successful Internet based companies are in a continual state of renewal always adapting to the ebb and flow of consumer demand. Our regulatory framework must match this dynamism.

2. Consumer Data Privacy Issues To Address Through Enforceable Codes of Conduct

I. Background

On February 23, 2012 the White House released "Consumer Data Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."[3] This report establishes a new consumer privacy framework entitled the "Consumer Privacy Bill of Rights." Among the stated goals of the framework is to provide ". . . data privacy protections . . . essential to maintaining consumers' trust in the technologies and companies that drive the digital economy."[4] In addition, the report " . . . urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights."[5]

[3] Available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[4] *Id*., at 1.
[5] *Id*., at 35.

Subsequently, on March 26, 2012 the Federal Trade Commission (FTC) issued its report entitled "Protecting Consumer Privacy in an Era of Rapid Change."[6] In the report, the FTC highlighted that for " . . . the last 40 years, the [agency] has taken numerous actions to shape the consumer privacy landscape."[7] In 1998, the FTC published "Privacy Online: A Report to Congress."[8] In this report, the FTC articulated the concept of the Fair Information Practice Principles (FIPPs) comprised of notice, choice, access and security as an appropriate self-regulatory framework for protecting online privacy.[9]

Since then, the FTC has continued to study the issue through surveys, research and public comments, conferences, and workshops. More recently, the FTC stated that it conducted a series of roundtables entitled "Exploring Privacy" between December 2009 and March 2010. The themes that are constant in these efforts is a recognition that the self-regulatory FIPPs framework has been critical to protecting consumer online privacy, that it is focused on the behavior of the actor and not the technology, and that the Internet is in a continual state of change that challenges policy makers to keep pace.

Notwithstanding, the most recent report entitled "Protecting Consumer Privacy in an Era of Rapid Change" reported that commentators raised several drawbacks to the FIPPs framework. First, that "the notice-choice model . . . led to long, incomprehensible privacy policies that consumers typically do not read."[10] Second, that "the harm-based model . . . had been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored."[11]

The FTC stated that "participants noted that both of these privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers."[12]

---

[6] Available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[7] *Id*. at ii.
[8] Available at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
[9] *Id.* at i.
[10] *Supra,* White House at 2.
[11] *Id.*
[12] *Id.*

II. Preserving a Self-Regulatory Model for Protecting Consumer Privacy and Fostering Innovation

In all of the aforementioned privacy reports, including the "Framework for Consumer Privacy" or the numerous FTC reports on privacy there have been scant discussions or studies focused on the benefits derived from a self-regulatory model.[13] More importantly, there has been no mention that most of recent and emerging Internet based companies that are transforming our world have fostered and thrived under the FIPP self-regulatory regime, and consumers have benefited immensely by the wealth of information and range of goods of services they have received via the Internet.

The fact that the FIPP's have not been able to "keep pace with the rapid growth of technologies. . ." is the reason why a self-regulatory approach to protecting consumer privacy is the most appropriate model.[14] If public policies around privacy were not able to keep pace with Internet based technologies twenty years ago when the technology was in its infancy why should the industry expect new privacy public policies to keep up with technology any better today when the technology is evolving faster than ever. The problem with regulations that are etched in stone is that they take a snapshot of the environment in a point in time without a mechanism for responding to a rapidly changing environment that is always looking for new ways of creating and offering services over the Internet.

The United States struck the right balance by requiring a self-regulatory approach to privacy while ensuring accountability from companies to meet their privacy commitments to consumers. As a result, the United States can boast of the start of not only new global companies, but also entirely new Internet platforms such as social networking. A self-regulatory model that is based on an FIPP framework will continue to foster new Internet based technologies that are innovative, and responsive to consumer demand.

[13] Supra, FTC 2012 Privacy Report.
[14] *Id*.

CompTIA respectfully suggests that NTIA should study and report on whether a self-regulatory model or a legislative mandate model is more appropriate to ensuring consumer privacy while also promoting innovation in the Internet economy.

A. The Enforceable Promises Regime Works Without the Need for Codifying Privacy Legislation

In 2001, then FTC Secretary Timothy Muris stated that privacy policies posted on commercial websites were "enforceable promises" under Section 5 of the Federal Trade Act..[15] As companies adopt these policies they continue to serve as enforceable promises under Section 5.. For example, FTC Privacy Report[16] in the era of rapid change it highlighted the numerous enforcement actions it successfully litigated against companies found to have violated its posted privacy statements.

Companies should be held responsible for the promises they make to consumers. However, in the same way that commentators have noted that the "notice-choice" and the "harms-based" models are no longer adequate to protect consumer privacy we believe that any privacy legislation will become out of date in the same way. Instead, CompTIA supports a self-regulatory model comprised of FIPP's as enforceable promises to provide accountability over how companies collect, store, share, and transmit personally identifiable information.

Consumer demand is the driving force behind any successful business model. Companies that fail to gauge and/or respond to the needs of their consumers are doomed to fail. Companies that suffer reputational and brand damage lose customers, market share, profits, and ultimately go out of business.

[15] Supra, note 2.
[16] *Id.*

CompTIA respectfully suggests that NTIA should study and report whether the aforementioned enforceable promises framework has protected consumer privacy while allowing continued innovation in the Internet economy.

B. Transparency and Context Are Important Additions to a Self-Regulatory Framework of FIPP

The Administration's "Framework for Protecting Privacy . . ." introduces the Consumer Privacy Bill of Rights which include the concepts of (1) Individual Control, (2) Transparency, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability.[17] All of these concepts are important and are outgrowths of the Fair Information Practice Principles.

CompTIA believes that these concepts are a reflection of more dynamic technologies used by entities that collect consumer information. For example, many of the complaints raised by consumers center on lack of transparency as to how personally identifiable information is used and notably how their information is disclosed to third parties.

CompTIA supports the Consumer Privacy Bill of Rights, but not as a static model that stands still in time. Instead, the Consumer Bill of Rights should serve as guideposts and best practices to be adopted by the industry. Moreover, a self-regulatory approach ensures accountability for the industry under not only Section 5 of the Federal Trade Commission Act, but also under numerous state specific consumer protection statutes that protect consumers against unfair trade practices.

CompTIA respectfully suggests that NTIA report on the feasibility of expanding the FIPP framework to incorporate the Consumer Privacy Bill of Rights as a set of self-regulatory best practices that can also serve as enforceable promises.

[17] *Supra*, White House Report.

IV. Mobility, Industry Best Practices, and Certifications

The development of growth of mobile applications is radically changing how people communicate, share information, and engage in e-commerce. Nevertheless, this industry is still in its infancy. CompTIA is concerned that any attempts to impose regulations will stifle further innovation and growth of these very important sector. A more suitable approach to improving the privacy practices of mobile app development firms is for federal agencies to work with the industry to develop benchmarks and best practices. For example, a CompTIA member company, "viaForensics," has submitted comments in these proceedings identifying some of the vulnerabilities associated with mobile devices and a set recommended best practices. CompTIA strongly favors this approach.

Moreover, it is CompTIA's experience that the IT industry has a natural evolution that starts with the development of best practices which then mature into industry led certification efforts. This process should be voluntary and the marketplace should decide which certifications provide the greatest consumer value. For example, CompTIA has over 1.5M IT vendor neutral workforce certifications out in the field, which were developed in a self-regulatory environment by IT firms and businesses that sought to create a better trained IT workforce.

3. Closing Remarks

CompTIA applauds the Department of Commerce and NTIA for its leadership in undertaking the very important task of identifying ways to create a more productive multistakeholder process, as well as seeking suggestions for relevant and timely privacy topics. As a not-for-profit organization that represents over 2,000 small and medium size businesses CompTIA is very interested in working with federal agencies, such as the Department of Commerce, the National Telecommunications and Information Administration to develop solutions to the important issues raised in the RFC.

David Valdez

Senior Director,

Computing Technology Industry Association

515 2nd St NE

Washington, DC 20002

(202) 441-3292

dvaldez@comptia.org