

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Preserving the Open Internet)	GN Docket No. 09-191
)	
Broadband Industry Practices)	WC Docket No. 07-52

COMMENTS OF THE FUTURE OF PRIVACY FORUM

Jules Polonetsky
919 18th Street, NW
Washington, DC 20036
(202) 713-9466
julespol@futureofprivacy.org

Christopher Wolf
Mark W. Brennan
HOGAN & HARTSON LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-8834
(202) 637-5910 (fax)
cwolf@hhlaw.com
Counsel for THE FUTURE OF PRIVACY FORUM

January 14, 2010

TABLE OF CONTENTS

	<u>Page</u>
Executive Summary	i
I. INTRODUCTION	1
II. ABOUT THE FUTURE OF PRIVACY FORUM.....	2
III. BROADBAND USE IMPLICATES SUBSTANTIAL PERSONAL PRIVACY CONCERNS.....	4
A. The Collection, Use, Sharing, Security, and Disposal of Personal Information Occurs at Many Places on the Internet	5
B. The Collection, Use, Sharing, Security, and Disposal of Personal Information Raises Invasion of Privacy, Identity Theft, Transparency, and Discrimination Concerns	7
C. Next-Generation Networks Will Create New Data Security and Privacy Risks	9
IV. THE FCC SHOULD CLARIFY THAT BROADBAND SERVICE PROVIDERS HAVE FLEXIBILITY TO DEPLOY INNOVATIVE TOOLS THAT ENHANCE CONSUMER PRIVACY AND DATA SECURITY.....	11
V. CONCLUSION.....	15

EXECUTIVE SUMMARY

Broadband access and use implicates numerous privacy and data security issues. The privacy focus of this proceeding has been on ensuring that broadband Internet access service providers do not interfere with user privacy rights, an important goal. Equally important, the Commission should ensure that any new rules it adopts in this proceeding do not impair broadband Internet access service providers' ability to empower consumers and deploy innovative tools to protect consumer privacy online.

The collection, use, sharing, security, and disposal of personal information occurs at many places on the Internet and often involves numerous parties in the broadband ecosystem. These activities create risks to consumers such as identity theft, and they raise concerns about the unwanted distribution of personal information to unintended recipients. Moreover, with the development of next-generation all-IP networks, broadband communications are transitioning to a more open technology environment. Although these networks will provide opportunities for many exciting new services and applications, they also portend new privacy and data security risks for consumers.

Consumers only will expand their adoption and usage of broadband services and technologies if they can be confident that there are adequate privacy and data security protections available. Thus, ensuring that broadband Internet access service providers can deploy innovative tools to protect consumers' personal information and respond to evolving security risks is a critical element in promoting an open Internet and facilitating broadband use.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Preserving the Open Internet)	GN Docket No. 09-191
)	
Broadband Industry Practices)	WC Docket No. 07-52

COMMENTS OF THE FUTURE OF PRIVACY FORUM

I. INTRODUCTION

The Future of Privacy Forum (“FPF”) submits these Comments regarding the Federal Communications Commission’s (“FCC’s” or “Commission’s”) October 22, 2009 Notice of Proposed Rulemaking (“*NPRM*”) in the above-referenced proceeding.¹ In the *NPRM*, the Commission seeks to “preserve an open Internet” in a manner that, among other things, “will protect the legitimate needs of consumers.”² To achieve its goal, the Commission proposes to codify its four existing Internet policy principles and add new nondiscrimination and transparency principles.³

As discussed below and as recognized by the Commission, broadband access and use implicates numerous privacy and data security issues. The focus thus far has been on ensuring that broadband Internet access service providers respect user privacy. Equally important, the Commission should ensure that broadband Internet access service providers can protect consumers’ personal information and provide adequate privacy and security for that information. Such protection is a vital component of promoting an open Internet and facilitating broadband

¹ *Preserving the Open Internet, Broadband Industry Practices*, Notice of Proposed Rulemaking, 24 FCC Rcd 13064 (2009) (“*NPRM*”).

² *Id.* ¶¶ 2, 10.

³ *Id.* ¶ 11.

use. Therefore, the Commission should make sure that any new rules it adopts in this proceeding do not impair service providers' ability to empower consumers and deploy innovative tools to protect consumer privacy.

II. ABOUT THE FUTURE OF PRIVACY FORUM

FPF is a Washington, DC-based think tank founded in late 2008 whose purpose is to examine current and emerging challenges to personal privacy and to propose practical ideas to improve personal privacy now and in the future.⁴

As an example of FPF's work, FPF currently is engaged in a project to design new forms of timely, informative, and eye-catching privacy notices concerning the collection of personal information for targeted advertising online. As the Federal Trade Commission ("FTC") has emphasized, consumers deserve to be better informed about the online collection of personal information for advertising purposes so that they can make choices about how that information is used. In that connection, the FTC expressed concern early last year that privacy policies were not being read or understood by consumers, and it urged the industry to develop new ways to notify consumers about online data collection and use. With this in mind, FPF partnered with a global marketing communications company to launch a consumer-focused effort that would rely on the skill of advertising and communications professionals to produce notices accessible through symbols or "icons." The icons were tested with an Internet survey of a large group of users to determine their utility in providing effective notice, and to select the most effective

⁴ FPF is supported by AOL, AT&T, The Better Advertising Project, Deloitte, eBay, Facebook, Intel, Lockheed Martin, Microsoft, The Nielsen Company, Verizon, and Yahoo! It has an advisory board of leading privacy advocates from business, law, non-governmental organizations, and academia. About the Forum, Future of Privacy Forum, *at* <http://www.futureofprivacy.org/about-the-future-privacy-forum/> (last accessed Jan. 14, 2010). The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

symbols and language. The icons and associated language that were selected already have been deployed for testing by Yahoo! and AT&T, and they are being considered for adoption as part of the self-regulatory programs of a coalition of leading industry groups. Thus, FPF has taken a leadership role in the undertakings urged by the FTC.

Another major FPF initiative concerns privacy and the Smart Grid. As the Commission is aware, modernization efforts are underway to make the current electrical grid “smarter” through the collection of data about consumer usage. FPF is taking the lead here as well, working with the GridWise Alliance, the Privacy Commissioner of Ontario, and others to address the potential privacy concerns implicated by the Smart Grid and to propose that privacy protections be built into the Smart Grid network as it is developed, using the principles of “Privacy by Design.”⁵

Finally, among the major ongoing FPF initiatives, FPF is focusing attention on the data collection issues raised by the growing popularity of Internet-based applications, or “apps,” especially those supported by social networking platforms and by mobile devices. FPF has been advocating that users be provided with sufficient and timely information by app developers so that users can understand how data about them may be used when they interact with apps. FPF is also urging app developers to be transparent about their data practices.

As the name suggests, FPF is focused on privacy issues that loom large for the future, which is why it makes this submission in connection with the Commission’s focus on the preservation of an open Internet.

⁵ FPF filed comments urging the Commission to encourage responsible data management practices by all entities involved in the Smart Grid ecosystem and facilitate stakeholder discussions to develop best practices. Comments of the Future of Privacy Forum – NBP Public Notice #2, GN Docket No. 09-47 (filed Oct. 2, 2009) (“*Smart Grid Comments*”); *see also* Comments of the Future of Privacy Forum, Report to the National Institute of Standards and Technology on the Smart Grid Interoperability Standards Roadmap, Department of Commerce, Docket No. 0906181063-91064-01 (filed July 30, 2009).

III. BROADBAND USE IMPLICATES SUBSTANTIAL PERSONAL PRIVACY CONCERNS

As the Commission previously acknowledged in its National Broadband Plan proceeding, “Americans are using broadband to perform everyday tasks in which they pass personal and confidential information over broadband connections, raising important consumer privacy concerns.”⁶ Today, consumers access the Internet to pay bills; maintain bank accounts; file taxes; communicate via e-mail, blogs, instant messaging, and social networking sites; purchase clothing, household goods, and entertainment items; read newspapers; conduct research on personal issues, including politics, legal matters, health and welfare, and finances; and receive remote healthcare monitoring.⁷

In addition to streamlining consumers’ lives, the use of these convenient services and applications also produces secondary benefits that enhance consumers’ online experience. Through the collection of consumer data, companies provide users with customized online experiences that include personalized content and targeted advertisements. When provided with appropriate transparency and control, such personalization can be relevant and responsive to consumers’ needs, generate increased business revenues, and subsidize free online content.⁸ As broadband services become available in more areas, companies will have additional opportunities to develop new business models, improve data collection technologies, create new services and applications, and personalize consumer content further.

⁶ *A National Broadband Plan for Our Future*, Notice of Inquiry, 24 FCC Rcd 4342 ¶ 58 (2009) (“*Broadband Plan NOI*”). FPF filed comments in response to the *Broadband Plan NOI*. Comments of the Future of Privacy Forum, GN Docket No. 09-51 (filed June 8, 2009).

⁷ See *Broadband Plan NOI* ¶ 58, n. 85; see also Jordan McCollum, *Study Looks at Internet Use in America*, WEBPRONNEWS (Jan. 2, 2008), at <http://www.webpronews.com/topnews/2008/01/02/study-looks-at-internet-use-in-america> (last accessed Jan. 14, 2010).

⁸ See Future of Privacy Forum Mission, at <http://www.futureofprivacy.org/2008/11/15/the-future-of-privacy/> (last accessed Jan. 14, 2010).

Along with the benefits of advanced data sharing, however, come significant challenges. The changing marketplace will encourage businesses to delve more deeply into data that can be used to make more efficient and effective marketing decisions.⁹ Moreover, the attendant risks of data sharing not only raise questions regarding how companies will continue to collect, combine, and disclose consumer data, but also raise critical consumer privacy concerns.

A. The Collection, Use, Sharing, Security, and Disposal of Personal Information Occurs at Many Places on the Internet

As explained in a 2009 TRUSTe report, the collection, use, sharing, security, and disposal of consumers' personal information occurs online at the many Web sites that consumers visit on a regular basis.¹⁰ In addition, the data collections are not only used by those Web sites, but are also shared with a variety of third parties in the broadband ecosystem, including but not limited to vendors, intermediaries, content providers, ad networks, affiliates, exchanges, and data analytic firms.¹¹ These parties also collect and share non-personally identifiable information related to consumers by tracking their online activity. To carry out these first-party data collection and third-party data sharing activities, companies rely on users' IP addresses, cookie IDs, ad tags, pixel tags, Web beacons, account IDs corresponding to registered users, log files, and other data.¹² Generally, these technologies permit companies to either recognize the user's browser or direct a user's browser to present itself to servers so data about the user's online activity at one site or across many Web sites can be used or personalized content and

⁹ *Id.*

¹⁰ TRUSTe, *Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust*, 4 (Feb. 2009), available at <http://www.truste.com/resources/index.html> (last accessed Jan. 14, 2010) ("TRUSTe WhitePaper").

¹¹ *Id.*

¹² *Id.* at 12-13 (describing the technological tools Web sites and third parties employ to collect and transfer data originating from the consumer's Web activity and ending with the ad network, data analytics firm, or the like).

advertisements can be delivered.¹³

Behavioral advertising is a contemporary example of personal data collection through such technologies and how anonymous information can be used to tailor advertising and marketing messages. According to the FTC, “[o]nline behavioral advertising involves the tracking of consumers’ online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience.”¹⁴

One such example of online tracking includes companies’ use of cookies placed on the consumer’s computer. To illustrate, upon researching hotels in Las Vegas, the Web site viewed by a user may display banner advertisements for a local hotel (or a hotel company with locations in Las Vegas). Here, the Web site or third party ad network recognized the unique cookie on the consumer’s Web browser, which enabled the data collector to correlate data about Web sites visited, banners clicked on, or search terms entered at other sites in its network.¹⁵

The collection of consumers’ personal data for the purposes of behavioral advertising also can be used in conjunction with other forms of targeting based on factors like geography, demographics, the surrounding content, or offline information. Activities such as data mining, so-called deep packet inspection advertising, consumer profiling, and location-based tracking through mobile devices allow companies to take advantage of consumers’ personally identifiable

¹³ *Id.*

¹⁴ Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*, 2 (Feb. 2009) (“FTC Principles”); *see also* TRUSTe Whitepaper at 5-7 (noting that the range of behavioral uses includes tailoring advertisements on a Web site to a certain consumer or consumer groups, tailoring advertisements across Web sites commonly owned by a company, providing data to an ad server to target advertisements for a specific publisher, tracking for analytics research, and making data available to third parties via an ad exchange for unlimited use or to an ad network for use on other sites).

¹⁵ *See* FTC Principles at 2 (describing how a network advertiser places and uses a cookie on a consumer’s computer to deliver targeted advertisements).

and non-identifiable information (“PII” and “non-PII,” respectively) to provide commercial information to them. While the information gathered by advertising networks is often not explicitly personal, consumers’ online activities across Web sites can be combined to create consumer profiles, and such profiles can then be enhanced by merging them with offline data or with PII.¹⁶

B. The Collection, Use, Sharing, Security, and Disposal of Personal Information Raises Invasion of Privacy, Identity Theft, Transparency, and Discrimination Concerns

Although many consumers may appreciate the personalized online experience provided by behavioral advertising and other online data collection processes, there are privacy issues that must be navigated to offer users this experience responsibly. For example, there is a concern that sensitive information regarding health, finances, certain demographics, or children could fall into the “wrong hands or be used for unanticipated purposes.”¹⁷ According to a 2009 press release, TRUSTe learned from surveys that 51 percent of consumer respondents worry about protecting their private information online.¹⁸ Thus, many consumers are uncomfortable that the disclosure of financial or other sensitive information may result in an invasion of their privacy, identity theft, credit card theft, or the unauthorized sharing of health and financial records.¹⁹

¹⁶ See, e.g., Federal Trade Commission, *Online Profiling: A Report to Congress*, 7-8 (June 2000), available at <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> (last accessed Jan. 14, 2010).

¹⁷ FTC Principles at ii.

¹⁸ Press Release, TRUSTe, Behavioral Advertising: Not that Bad?! TRUSTe Survey Shows Decline in Concern for Behavioral Advertising – Consumers Want Relevant Ads Online, But Still Worry About Their Online Privacy (Mar. 4, 2009) (“TRUSTe Survey”), available at http://www.truste.com/about_TRUSTe/press-room/news_truste_survey_shows_decline_concern_for_ba.html (last accessed Jan. 14, 2010).

¹⁹ *Id.* (listing that of the consumer respondents, 35% felt that their privacy was violated due to information they provided over the Internet; 6% reported having their identity stolen in 2008; 11% experienced credit card theft in the last year; and 13% reported unauthorized sharing of highly sensitive personal information over the last year).

In addition, some consumers may not fully understand (or may be unable to control adequately) online data collection practices and how their information is being used by those providing broadband services. In practice, many Web site privacy policies and opt-out mechanisms are not easily understood and have the potential for consumer confusion. Moreover, the variety of technologies used for online tracking are not always disclosed to or readily understood by the consumer.²⁰ Consequently, consumers often are not fully informed as to who is collecting the data, cannot see all the information that is being collected about them, and do not have the ability to access or control the profiles that marketers have compiled.²¹

Technological solutions to these challenges are being developed to empower consumers to better control and adjust their online privacy environment in real time, much as they do in the real offline world, where for example an individual will visit his or her doctor and then afterwards buys groceries in a busy supermarket. The individual's behavior, expectation of privacy, and personal privacy shields will change as the individual steps out of the doctor's office and into the busy supermarket, where the individual may prefer to remain anonymous. The idea of empowering broadband users to adjust their privacy shields and identity profiles in real time in the online world is at the heart of numerous technological innovations, not only at the edges of networks but also at the core. These innovative solutions should be encouraged, and

²⁰ Consumers may believe that certain online activity is anonymous. However, there is the potential that such information could be aggregated and linked by a common identifier. The resulting "highly detailed and sensitive profile" could then be traced to the consumer or combined with "even richer, more sensitive, data" to identify that consumer, and it could even be used against the consumer for unlawful or discriminatory purposes. *See, e.g.*, FTC Principles at 22-23.

²¹ *See, e.g., id.* at 30-37 and Concurring Statement of Commissioner Pamela Jones Harbour, 3-4 (Feb. 2009). The collection of online data related to children, moreover, raises numerous privacy concerns. Children have proven to be early adopters of Internet and wireless technologies and are often more proficient than their parents in using computers, mobile devices, MP3 players, and game consoles. Because children are such avid Internet users, some advocacy groups have become increasingly concerned about advertisers targeting children online.

not hampered by any rules developed by the Commission in the context of this proceeding.

C. Next-Generation Networks Will Create New Data Security and Privacy Risks

Broadband Internet services and applications are on the verge of a new era. With the development of all-Internet Protocol (“IP”) next-generation networks (“NGNs”), broadband communications are transitioning to a more open technology environment. Whereas the existing circuit-switched public switched telephone network (“PSTN”) is an essentially closed system that provides network operators full control over all service interfaces, NGNs are being designed around converged networks and services that utilize open architectures and rely entirely on common IP-based technologies. Although NGNs will provide opportunities for many exciting new services and applications, they also portend new privacy and data security risks for consumers.

The development of NGNs is spurring innovation in all network segments, including at both the network edge and core, and NGNs are expected to enable the emergence of a broad array of new applications and services. In addition, the networks will include advanced features such as ubiquitous, real-time, multimedia communications; enhanced network management capabilities; greatly expanded user customization and information filtering; and more context-sensitive user interfaces. The number of Internet-enabled devices is also expected to surge as NGNs are deployed. As one example of an NGN, Smart Grid systems increase the connectivity, automation, and coordination of energy transmission and distribution between suppliers, networks, and consumers. Smart Grid technology also can expand energy efficiency into the home by monitoring consumers’ energy usage in real time and communicating with household devices that respond to demands to shut off during periods of non-use (*e.g.*, during the work day, when businesses require more power resources), allowing individual consumers to

control their electricity usage more effectively.²²

Despite its benefits, the open NGN architecture will also create new risks for consumers. Specifically, new threats will arise as part of the transition to these all-IP networks due to the shared core network infrastructure, the large number of gateways and other connectivity points with the public Internet, and new remote access capabilities. New customer equipment can also pose risks as more third-party applications become available through “app stores” and other sources in the broadband ecosystem. Thus, the equipment itself can become a vessel for viruses, malware, and malicious code targeting the equipment user, network operator, or other network users. Users may also be able to manipulate their equipment for service and identity theft, billing fraud, and other unlawful purposes. Absent creative, effective network management solutions by broadband Internet access service provider to thwart these activities (and the unknown threats of the future), the number of data security breaches is expected to rise dramatically as NGNs are deployed.

²² As FPF explained in its *Smart Grid Comments*, Smart Grid technology can expand energy efficiency into the home by monitoring consumers’ energy usage in real time and communicating with household devices that respond to demands to shut off during periods of non-use (e.g., during the work day, when businesses require more power resources), allowing individual consumers to control their electricity usage more effectively. However, the opportunities and benefits of developing Smart Grid systems also come with potential privacy risks.

Potential Smart Grid data users, including utility companies and device manufacturers, must engage in responsible data management practices that build consumer confidence and trust. They must also recognize that they have an ongoing relationship with consumers and that continued trust from consumers is critical to maintaining that relationship and to growing the Smart Grid ecosystem. Such trust can only be achieved if consumers feel that they are receiving sufficient information about and are in control of how their personal Smart Grid data is used. Thus, Smart Grid data users must consider carefully how they will protect the integrity, privacy, and security of the Smart Grid data obtained from consumer usage patterns. In addition, Smart Grid data must be gathered responsibly, securely, and with a measure of transparency and consumer control. See *Smart Grid Comments* at 3-4.

IV. THE FCC SHOULD CLARIFY THAT BROADBAND SERVICE PROVIDERS HAVE FLEXIBILITY TO DEPLOY INNOVATIVE TOOLS THAT ENHANCE CONSUMER PRIVACY AND DATA SECURITY.

Broadband service providers should recognize that ensuring adequate privacy and data security protection is a critical service provided to their customers. Numerous applications, services, and other content available through broadband Internet access services rely heavily on the collection, communication, and storage of data from consumers. As discussed above, although this data can be used to enhance consumers' online experience and provide customized benefits for users, it could also be used improperly to gain detailed insight into consumer behaviors, habits, activities, and lifestyles. Broadband Internet access service providers therefore will need to continue providing consumers with innovative tools to enhance data security and user privacy, and the FCC should clarify that "reasonable network management" encompasses these activities.

In the *NPRM*, FCC proposes rules that would restrict the ability of broadband Internet service providers to:

- prevent users from sending or receiving the lawful content of the user's choice over the Internet;
- prevent any users from running the lawful applications or using the lawful services of the user's choice;
- prevent any users from connecting to and using the user's choice of lawful devices that do not harm the network; and
- deprive any users of the user's entitlement to competition among network providers, application providers, service providers, and content providers.²³

In addition, the FCC proposes rules that would require broadband Internet service providers to:

- treat lawful content, applications, and services in a nondiscriminatory manner; and
- disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the other open Internet protections.²⁴

²³ *NPRM* at Appendix A.

²⁴ *Id.*

All of the proposed rules would be subject to “reasonable network management,” which the FCC proposes to define as: (a) reasonable practices employed by a provider of broadband Internet access service to reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; address traffic that is unwanted by users or harmful; prevent the transfer of unlawful content; or prevent the unlawful transfer of content; and (b) other reasonable network management practices.²⁵

As the Commission considers adopting new rules to promote an open Internet, it must be careful not to impair the ability of broadband Internet access service providers to empower consumers with tools to protect their online privacy. More and more service providers are actively competing to implement responsible data management practices that build consumer confidence and trust. For certain services and applications, moreover (*e.g.*, eHealth), privacy concerns are paramount. In addition, as NGNs are deployed, broadband Internet access service providers may need to deploy network-based, privacy-driven barriers to protect consumers against activities or third-parties, moving beyond the filtering and monitoring services available today. Such tools could include providing anonymity tools, helping maintain consumer opt-outs or other privacy preferences, and collaborating with social networking platforms, mobile device makers, and application developers to support responsible uses of consumer data. As the FTC acknowledged in a 2007 Staff Report, some of the same technologies that have been criticized for “discriminating” against certain traffic “can be and are used to improve network security by

²⁵ *Id.*

identifying and protecting the network against viruses, spyware, and other dangers to the system.”²⁶

Given the need for rapid, dynamic responses to evolving privacy and data security threats, any rules designed to preserve an open Internet must ensure that service providers can deploy truly privacy-enhanced online environments as part of their “reasonable network management” activities. In addition, the Commission’s open Internet rules should in no case hamper innovation and investment in privacy-enhanced online environments, regardless of whether the privacy enhancing technology and services are developed at the edge or at the core of networks.

FPPF believes that the “reasonable network management” provision in the Commission’s draft rules encompasses actions that further privacy and data security goals. For example, “reasonable network management” is defined to include actions that “reduce or mitigate the effects of congestion,” “address quality-of-service concerns,” “address traffic that is unwanted by users or harmful,” and “other reasonable network management practices.”²⁷ The Commission also clarified that in the *NPRM* that actions to address harmful traffic or traffic unwanted by users could include blocking spam and malware or malicious traffic originating from malware.²⁸ However, to remove any doubt, the FCC should consider expanding the definition of “reasonable network management” to include an explicit provision for actions that enhance user privacy and data security. In this way, the Commission can promote highly secure online activities and encourage broadband Internet access service providers to compete vigorously to provide the best privacy tools and secure online experience for consumers. Only if consumers have confidence

²⁶ Federal Trade Commission, *FTC Staff Report: Broadband Connectivity Competition Policy*, 135 (June 2007).

²⁷ *NPRM* at Appendix A.

²⁸ *Id.* ¶ 138.

about their online privacy will there be continued explosive growth in broadband Internet services.

In addition to broadband Internet access services, to which the Commission proposes to apply the six rules described in the *NPRM*, the Commission mentions “managed and specialized services,” which could be either excluded from regulations or subject to other, presumably lighter, regulation. The managed or specialized services mentioned by the Commission include services where privacy concerns are paramount, such as telemedicine or smart grids.²⁹ To the extent the Commission sets out criteria to identify “managed or specialized services” and distinguish them from broadband Internet access services, one of the criteria should be the existence of a managed end-to-end quality of service environment that incorporates specific privacy and/or identity management functions. If the Commission decides to impose some form of regulation on managed or specialized services, it should ensure that its regulations support the development of innovative privacy and identity management solutions.

²⁹ *Id.* ¶ 150.

V. CONCLUSION

For the foregoing reasons, the Commission should ensure that any new rules it adopts in this proceeding do not impair broadband Internet access service providers' ability to empower consumers and deploy innovative tools to protect consumer privacy online.

Respectfully submitted,

/s/ Christopher Wolf

/s/ Jules Polonetsky

Jules Polonetsky
THE FUTURE OF PRIVACY FORUM
919 18th Street, NW
Washington, DC 20036
www.futureofprivacy.org
(202) 713-9466
julespol@futureofprivacy.org

Christopher Wolf
Mark W. Brennan
HOGAN & HARTSON LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-8834
(202) 637-5910 (fax)
cwolf@hhlaw.com
Counsel for THE FUTURE OF PRIVACY FORUM

January 14, 2010