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

REPLY COMMENTS OF THE FUTURE OF PRIVACY FORUM

I. INTRODUCTION

The Future of Privacy Forum ("FPF"), a think tank whose mission is to advance the protection of personal data,[1] submits these Reply Comments regarding the Federal Communications Commission's ("Commission") October 22, 2009 Notice of Proposed Rulemaking ("*NPRM*") in the above-referenced proceeding.[2] In its initial Comments,[3] FPF advocated that broadband Internet access service providers ("providers") not be restricted in their ability to protect consumers' personal information. Specifically, FPF requested that any new rules adopted by the Commission not impair providers' ability to deploy innovative tools to protect consumer privacy online, including tools that will empower consumers to protect their own personal information. In these Reply Comments, FPF provides additional information

---

[1] *See About the Forum*, Future of Privacy Forum, *at* http://www.futureofprivacy.org/about-the-future-privacy-forum/ (last accessed Apr. 26, 2010). The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

[2] *Preserving the Open Internet, Broadband Industry Practices*, Notice of Proposed Rulemaking, 24 FCC Rcd 13064 (2009) ("*NPRM*").

[3] Comments of the Future of Privacy Forum, GN Docket No. 09-91 (filed Jan. 14, 2010) ("FPF Comments").

regarding the privacy and data security risks that loom on the horizon with next-generation networks ("NGN") and the need for creative, effective network management solutions to thwart these risks.

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

As FPF previously explained, 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.[4] The collection, use, sharing, security, and disposal of personal information occur at many places on the Internet and often involve 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. As the Commission considers adopting new rules to promote an open Internet, it must be careful not to impair the ability of providers to empower consumers with tools to protect their online privacy and keep data secure.

With the development of all-IP NGNs, broadband communications are transitioning to a more open technology environment. Whereas the existing circuit-switched public switched telephone network ("PSTN") and mobile networks (both GSM and CDMA) are essentially closed systems that provide 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. NGNs will enable the emergence of a broad array of new applications and services with advanced features such as ubiquitous, real-time, multimedia

[4] *See id*.

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, both on fixed and mobile networks.

Although NGNs will provide opportunities for many exciting new services and applications, they also portend new privacy and data security 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. Customer equipment itself can also become a vessel for viruses, malware, and malicious code targeting the equipment user, network operator, or other network users. Absent creative, effective network management solutions by providers to ward off these threats, the number of data security breaches is expected to rise dramatically as NGNs are deployed.

Recent actions by the Federal Trade Commission ("FTC") underscore the need for service providers and network operators to take steps to keep their networks secure. In February, the FTC warned almost 100 organizations (ranging in size from eight-person operations to large, publicly held corporation) that personal information about their customers, employees, or both groups had been transmitted to and was available on peer-to-peer ("P2P") file-sharing networks.[5] As a result of these transmissions, the personal information was available to all users of the P2P networks. In letters to the companies, the FTC reminded each company of its responsibility to protect personal information from unauthorized access, which includes "taking steps to control

[5] *Widespread Data Breaches Uncovered by FTC Probe: FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks*, FTC Press Release (Feb. 22, 2010), *available at* http://www.ftc.gov/opa/2010/02/p2palert.shtm (last accessed Apr. 26, 2010).

the use of P2P software" on the company network and on any service providers' networks.[6] Management of security threats to protect personal data, the importance of which the FTC has underscored, requires retaining the ability to exercise management.

In addition, the FTC on March 25 entered into a consent decree with Dave & Buster's, Inc. ("D&B") to settle allegations that D&B failed to take reasonable steps to secure sensitive personal information on its network.[7] D&B's failures allegedly allowed a hacker to access approximately 130,000 customer debit and credit card numbers and spawn hundreds of thousands of dollars in fraudulent charges.[8] Of note, the FTC criticized D&B for, among other things, its failure to: employ sufficient measures to detect and prevent unauthorized access to its network (*e.g.*, adequate intrusion detection systems and system logs); adequately restrict third-party service provider access to its networks; monitor and filter outbound traffic from its network; block the unauthorized export of sensitive personal information; and limit access to its computer networks through wireless access points.[9] Providers are well-positioned to provide security tools that would augment the kinds of company-based tools cited by the FTC as bedrock components of "reasonable security."

In the current regulatory environment in which companies holding and transmitting personal data are expected to do more to protect such data, providers will appropriately be called up to assist in such efforts. For example, in its package of reforms adopted in November 2009, the European Union significantly increased the security obligations of network operators with

---

[6] *Id.*

[7] *Dave & Buster's Settles FTC Charges it Failed to Protect Consumers' Information: More than 130,000 Customers' Credit or Debit Cards Compromised*, FTC Press Release (Mar. 25, 2010), *available at* http://www.ftc.gov/opa/2010/03/davebusters.shtm (last accessed Apr. 26, 2010).

[8] *Id.*

[9] *Id.*

regard to personal data, including personal data that can be accessed in terminal devices.[10] These reforms increase the responsibility on network providers to find solutions against the multiple threats that will accompany the widespread adoption of all-IP next generation networks.

In addition, providers can be expected to deploy network-based, privacy-driven barriers to protect consumers against certain harmful activities or from third-parties; privacy portals and data use "dashboards;" dynamic ID management; and other features with capabilities far more expansive and more closely integrated than the filtering and monitoring services available today. For example, to prevent third-parties from introducing malicious code or other security threats into networks or customer equipment, providers may need to conduct certain testing or certification activities or provide after-the-fact remediation.[11]

Providers also could have a role as trusted "data custodians" that can work with consumers to protect personal information online. Providers have a unique relationship with consumers and can help them manage their online profiles and cyberspace "identities" in a secure manner. Providers could also act as data mediators for enterprise customers and other organizations. For these efforts to succeed, however, providers will need the flexibility to develop customized solutions that can address individual privacy attitudes and varying data sensitivity.

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 providers can deploy truly privacy-enhanced online environments as part of their "reasonable network management" activities. In addition, any open Internet rules should in no case hamper innovation and

---

[10] Article 4 of the amended E-Privacy Directive, Consumer Rights Directive 2009/146/EC dated 25 November 2009.

[11] *See, e.g.*, Comments of AT&T Inc., GN Docket No. 09-191, 149, 172 (filed Jan. 14, 2010).

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. The Commission should also ensure that any rules do not restrict providers from assisting consumers, enterprise customers, and other organizations with managing their online data.

Although FPF believes that the "reasonable network management" provision in the Commission's draft rules encompasses actions that further privacy and data security goals,[12] the Commission should consider expanding the definition of "reasonable network management" to include an explicit provision for actions that enhance user privacy and data security.[13]

III. CONCLUSION

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

Respectfully submitted,

/s/ Christopher Wolf
/s/ Jules Polonetsky

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

[12] *See NPRM* at Appendix A.

[13] *See* FPF Comments at 13-14. In addition, if the Commission decides to impose some form of regulation on managed or specialized services, it should ensure that its regulations authorize service providers to support the development and deployment of innovative privacy and identity management solutions for those services. *Id.* at 14.

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

April 26, 2010