

Ex Parte: Network Management and Open Network Proceeding

**Before the
Federal Communications Commission**

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

Consumer Policy Solutions¹ and the National Consumers League² appreciate the opportunity to offer additional information to augment the record in the Federal Communication Commission Notice of Proposed Rulemaking *In the Matter of Preserving the Open Internet Broadband Industry Practices*. The focus of this information relates to the management role network providers fulfill to maintain a safe and secure network and the important benefit this role presents for their customers.

Consumers have a critical interest in the vital role Internet Service Providers have in protecting the security and integrity of the network. Consumers already online, as well as new users, rely on the safety of the network and network operators have an important responsibility in providing this protection. In order for consumers to continue their use of broadband services, and for non-users to adopt broadband, they must be confident of their

¹ Consumer Policy Solutions is a firm centered on addressing the interests of consumers and the marketplace.

² The National Consumers League, founded in 1899, is America's pioneer consumer organization. Our mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. For more information, visit www.nclnet.org.

safety and security online. While network operators provide the management necessary for network and consumer protection harms of known problems such as spam, hacking, and botnets, and the potential threat they pose to the entire network today, it is of great importance that network operators be able to continue to manage the online consumer experience and threats to the network.

The safety and security of the network should therefore be a top priority of the Commission. Regardless of the adoption of any non-discrimination principle, the Commission needs to ensure that network providers have the ability to protect the safety and security of their users. To accomplish this objective, the Commission should allow Internet Service Providers the maximum flexibility needed for ongoing management and protection of the network and the consumers they serve. Malicious actors must not be allowed to threaten the security of the network and the safety of its users.

Providing consumers with a stable and reliable network is an integral component to building a broadband network that serves everyone. Consumers need to be confident that their online transactions and personal information are safe, secure and private in order to adopt and retain their broadband service.

Consumer concern about online safety and security is a significant barrier to broadband adoption. In the FCC's report, "Broadband Adoption and Use in America," non-users indicated that one of the primary reasons for not using and adopting broadband is that

they are “worried about all the bad things that can happen if I use the Internet.”³ Among non-adopters, 57% responded that “It is too easy for my personal information to be stolen online” and 46% responded that “the Internet is too dangerous for children.”⁴ The study clearly defines non-adopters concern about their own safety and welfare on the Internet influencing their decision to reject the opportunity to adopt broadband.

Concern about the security of online users was highlighted in “Connecting America: The National Broadband Plan,” released by the Commission in March 2010. In the Executive Summary of the Plan, the connection between broadband adoption and user confidence in the security and safety of the network is apparent. In the recommendation for Public Safety and Homeland Security, the summary states: “To achieve these objectives, the plan makes recommendations to... promote cybersecurity and critical infrastructure survivability to increase user confidence, trust and adoption of broadband communications.”⁵

Clearly, if one goal of the Plan is to increase broadband adoption, current users and non-adopters must feel confident with the safety and security of their online experience.

Network managers continue to work diligently to maintain the integrity and security of their networks, and have offered tools and information to reassure their users.

³ John B. Horrigan, Broadband Adoption and Use in America, February 23, 2010, pages 27 and 30.

⁴ John B. Horrigan, Broadband Adoption and Use in America, February 23, 2010, page 32.

⁵ Connecting America: The National Broadband Plan, FCC, March, 2010, page XIV.

While there are effective tools and other resources available to help protect consumers, network providers also offer an invisible shield for their customers, working behind the scenes to maintain the safety and integrity of the network. Those intent on threatening the safety of the network and consumers, are always one step ahead and will figure out a way to compromise the network. In order to help consumers most effectively, ISPs need to have the leeway to address these threats.

On a daily basis, the network is subjected to hundreds of thousands of threats and, if unchecked by network providers, consumers would be more vulnerable to a multitude of malicious actions. Two major examples of online security and safety threats include spam and botnets. There is a rich history of occasions when network providers have effectively managed their networks to filter out spam messages. For example, Comcast has reported that they filtered out 500 million spam messages per day in 2008.⁶ This is but one example of many that reveal the importance of the providers' ability to have flexibility to respond to the safety and security needs of their customers, and the network.

Consumers increasingly rely, both knowingly and unknowingly, on their Internet Service Providers to reduce the threat of these malicious network hazards. More importantly, consumers can benefit when ISPs provide protection against malware and viruses by building firewalls and filtering at the network level. Restrictive network management provisions would create some uncertainty about what the ISPs can and cannot do to protect their users from these online threats.

⁶ Adrienne Kroepsch, "Lawmakers Gear Up For Another 'Net Neutrality' Debate," *Congressional Quarterly Today*, 2/8/08

Through the implementation of the National Broadband Plan, the Commission has the opportunity to ensure network providers continue to have an unfettered ability to protect their users from these online perils. Internet Service Providers should be provided the ability needed for ongoing management and protection of the network and the consumers they serve.

In conclusion, as the Commission develops policies in this proceeding, it should be mindful of any unintended regulatory consequences that would compromise the flexibility of ISPs to manage their networks for the safety of their users and the integrity of the network. The Commission should recognize the critical role of ISPs in protecting their users from network threats and provide maximum flexibility to providers to enable them to provide these protections. The Commission should defer to the expertise of the network providers and allow them to engage in reasonable and flexible network management for the safety and security of their customers and the entire network. A safe and secure network serves the interest of all users. Thank you for the opportunity to offer our remarks regarding consumers' interest in the safety and security of their online experience.

Submitted on behalf of,

/s/

Debra Berlyn
President
Consumer Policy Solutions
7207 Summit Avenue

/s/

Sally Greenberg
Executive Director
National Consumers League
1701 K Street, N.W. Suite 1200

Chevy Chase, MD 20185
202-436-4313
drberlyn@drberlyn.com

Washington, D.C. 20006
202-835-3323
sallyg@nclnet.org