

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

International Comparison and Survey)	GN Docket No. 09-47
Requirements in the Broadband)	
Data Improvement Act)	
)	
A National Broadband Plan)	GN Docket No. 09-51
For Our Future)	
)	
Inquiry Concerning the Deployment of)	
Advanced Telecommunications Capability)	
to All Americans in a Reasonable and)	
Timely Fashion, and Possible Steps to)	GN Docket No. 09-137
Accelerate such Deployment Pursuant to)	
Section 706 of the Telecommunications)	
Act of 1996, as amended by the Broadband)	
Data Improvement Act)	

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION
ON NBP PUBLIC NOTICE #29**

The National Cable & Telecommunications Association (“NCTA”)¹ hereby submits its comments in response to the Public Notice issued by the Commission in the above-captioned proceedings.²

In the Notice, the Commission seeks comment on questions raised in a recent letter filed by the Center for Democracy and Technology (“CDT”) in the National Broadband Plan

¹ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of high-speed Internet service (“broadband”) after investing over \$145 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to over 20 million customers.

² Public Notice, *Comments Sought on Privacy Issues Raised by the Center for Democracy and Technology*, NBP Notice # 29, DA 10-62 (rel. Jan. 13, 2010) (“Notice”).

proceeding about the use of personal information and privacy in an online, broadband world.³

The letter seeks further public comment on such areas as consumer expectations of privacy, the development of technologies to protect privacy, use of transactional data and service provider liability for third party applications on their platforms.

With a long history of protecting cable subscriber privacy, the cable industry regards the protection of our customers' privacy as a fundamental part of our relationship with our customers and central to the success of our businesses. Cable systems operate in a highly competitive marketplace, and their ability to succeed depends on winning and retaining the trust of those customers. And as new business models and new network technologies are developed, operators have ensured and will ensure that they are deployed in a manner that respects their customers' privacy.

Section 631 of the Communications Act, enacted in 1984, provides a comprehensive privacy framework for cable operators.⁴ The law:

- requires cable operators to provide annual written notice to consumers of the nature of personally identifiable information (“PII”) collected, including clearly and conspicuously describing how it is used, disclosed to others, and maintained;
- prohibits cable operators from collecting PII without prior customer consent, except as necessary to render service and detect service theft, and from disclosing PII without prior customer consent, except as necessary to render services or conduct other legitimate business activities related to rendering service;
- provides detailed requirements governing how subscriber records may be disclosed pursuant to court order;

³ Letter from Ari Schwartz, Vice President and COO, Center for Democracy and Technology, to Marlene H. Dortch, Secretary, Federal Communications Commission, Ex Parte Presentation, Docket No. 09-51, 09-47, 09-137, January 11, 2010.

⁴ 47 U.S.C. § 551.

- requires that subscribers be given access, at reasonable times and convenient locations, to all PII that is collected and maintained, and a reasonable opportunity to correct any errors in PII; and
- requires cable operators to take “such actions as are necessary” to prevent unauthorized access to PII, including destroying it if it is no longer necessary for the purposes for which it was collected and there are no pending court orders or requests for access to such information.

In addition, cable providers of digital voice service comply with the privacy protections of Section 222 of the Communications Act regarding customer proprietary network information (“CPNI”).⁵ Between Section 631 and Section 222, the cable industry already operates in an enforceable privacy framework that substantively embodies well-recognized fair information principles.⁶

The dynamic broadband ecosystem presents new challenges for protecting consumer privacy. Privacy and security controls related to broadband access have become the marketplace norm to protect consumers from malware, spyware, viruses and other privacy invasions.⁷ But nearly all modern communications technologies – without which broadband networks could not function effectively and efficiently – have a variety of features and attributes that could implicate privacy concerns if misused. Thus, CDT asks the right question at the outset: “what principles and standards should be considered to help articulate existing consumer expectations of privacy?”

NCTA believes that achieving and sustaining subscribers’ trust requires adherence to a privacy framework that addresses four principles: first, giving customers *control*; second,

⁵ 47 U.S.C. § 222; 47 C.F.R. Part 64, Subpart U.

⁶ Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”; http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

⁷ See e.g. *In the Matter of A National Broadband Plan for Our Future* (“NBP proceeding”), GN Docket No. 09-51, Comments of Time Warner Cable Inc. at 13, citing variety of privacy tools; Comments of Comcast Corporation at 25 (June 8, 2009).

providing *transparency* and *notice*; third, *safeguarding personal information*; and fourth, providing customers with *value*.⁸ We also believe that with regard to transactional data special care should be given to sensitive data, such as health or financial information, as well as protecting children online.

And given the complexities involved in a rapidly evolving Internet world, it is important for all industry stakeholders to work together to establish best practices and self-regulatory principles.⁹ NCTA and its members are committed to continuing to work constructively with public and private broadband stakeholders to promote self-regulatory ground rules.

CDT also asks “what can federal agencies do to help ensure that consumer expectations of privacy are met as new technologies platforms are developed?” As the Commission is aware, the Federal Trade Commission has been actively exploring privacy issues, holding workshops and issuing a staff report on self-regulatory principles in February 2009.¹⁰ Most recently, it has begun a series of roundtables featuring a cross-section of experts to explore the privacy challenges posed by technology and business practices that collect and use consumer data. The first roundtable, held in December 2009, focused on, among other things, the benefits and risks of information-sharing practices and consumer expectations regarding such practices. The FTC is convening a second privacy roundtable on January 28, 2010 to focus on how technology

⁸ See Testimony of Kyle McSlarrow, President and CEO, National Cable & Telecommunications Association, on Communications Networks and Consumer Privacy: Recent Developments, House Energy and Commerce Subcommittee on Communications, Technology and the Internet, April 23, 2009, at 3.

⁹ See *e.g.* *NBP proceeding*, Comments of Cox Communications, “Improving the U.S. Broadband Experience” (industry should establish “meaningful and transparent self-regulatory principles or best practices for broadband data security, privacy and online safety”), June 8, 2009; Comments of Time Warner Cable at 12 (Sept. 4, 2009); Comments of Comcast Corporation at 26 (June 8, 2009); Charter Communications, Ex Parte, “Providing Regulatory Clarity to Enable Ad-Supported Models”, Sept. 15, 2009.

¹⁰ “FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising,” February 2009. The FCC also has statutory privacy responsibilities under Section 222 of the Communications Act and has long recognized the importance of exploring privacy policy issues raised by the emergence of the Internet. *In the Matter of IP-Enabled Services*, Notice of Proposed Rulemaking, WC Docket No. 04-36 (rel. Mar. 10, 2004). NCTA has actively participated in these proceedings.

affects consumer privacy, including its role in both raising privacy concerns and enhancing privacy protections. The roundtable will discuss cloud computing, mobile computing, and social networking.¹¹

The FTC and FCC also can help raise awareness and educate consumers on how to create an Internet environment that addresses their individual privacy concerns. For example, one of the barriers to adoption of broadband services identified in this proceeding is fear by some consumers related to privacy and security online.¹² The national broadband plan should support adoption initiatives that seek to address this concern.

In general, NCTA believes the government should encourage a framework that strikes the appropriate balance between legitimate privacy concerns and promoting the tremendous value of online information for consumers – from websites to e-commerce to advanced applications and services – as well as for broader societal goals. Since consumer concerns vary and new services and technologies must respond in these unique contexts, it should rely on competitive market forces, existing safeguards and industry self-regulation to protect consumers’ privacy interests rather than further regulatory mandates. Such actions could impede further investment in broadband infrastructure by the private sector and constrain the development of innovative applications and content, thereby undermining the Commission’s broadband goals.¹³ In addition, broad restraints could impact the creation of job growth in this valuable economic sector.

¹¹ The FTC announced that the third and final roundtable to be held on March 17, 2010 will address such issues as how best to protect health data and other sensitive consumer information, including information about children and teens. Congress is also reviewing the adequacy of the legal and policy framework for protecting consumers’ privacy in light of the growth in online applications and services.

¹² See e.g. “Barriers to Broadband Adoption, A Report to the Federal Communications Commission,” The Advanced Communications Law & Policy Institute, New York Law School, Oct. 2009, at 14, citing Pew Internet & American Life Project data, Feb. 2008.

¹³ Behavioral advertising, for example, has many advantages for consumers. Instead of receiving a barrage of irrelevant ads, customers can receive information about products and services tailored to their specific interests. Moreover, advertising remains a critical way to fund content and services online, often for free. Thus,

The final area of inquiry in CDT's letter is whether companies that create new platforms for third party broadband applications, such as energy grid and health records, should somehow be responsible for privacy violations by those entities. In particular, it asks whether "holding the platform provider liable for the actions of third-party applications that violate basic privacy and security standards create incentives to ensure that consumer privacy is protected?" The notion that a service provider should be held liable for the actions of third party applications on its network is completely contrary to existing law and various privacy-related bills.

For example, section 512 of the Digital Millennium Copyright Act ("DMCA") limits the liability of service providers in circumstances where the provider engages in "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections."¹⁴ This "passive carrier" exemption, often borrowing the language of the DMCA, has become a standard feature of privacy-related bills such as the data security and spyware legislation considered in recent Congresses.¹⁵

advertising that is more relevant for the consumer is likely to be of more practical value to the consumer and will promote the continued expansion of new content and services.

¹⁴ 17 U.S.C. § 512; http://www.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000512----000-.html.

¹⁵ See, e.g., H.R. 2221, 111th Cong., 1st Sess (2009), § 2(e) ("Nothing in this section shall apply to a service provider for any electronic communication by a third party that is transmitted, routed, or stored in intermediate or transient storage by such service provider.") (data security) (passed by the House); S. 1178, 110th Cong., 2d Sess. (2007), § 3(f) ("Section 2 and subsections (a), (b), and (c) of this section do not apply to electronic communication of a third party stored by a cable operator, information service, or telecommunications carrier in the network of such operator, service or carrier in the course of transferring or transmitting such communication.") (same) (reported by Senate Commerce Committee); H.R. 964, 110th Cong., 1st Sess. (2007), § 3(e)(1) ("A telecommunications carrier, a provider of information service or interactive computer service, a cable operator, or a provider of transmission capability shall not be liable under this section to the extent that the carrier, operator, or provider transmits, routes, hosts, stores, or provides connections for an information collection program through a system or network controlled or operated by or for the carrier, operator, or provider") (spyware) (passed by the House). The CAN-SPAM Act provides that the term "initiate," when used in connection with a commercial email message, "shall not include actions that constitute routine conveyance of such message." 15 U.S.C. § 7702(9). As the Senate Committee

Moreover, it is simply not feasible, as a practical matter, for Internet Service Providers (ISPs) to police all of the content on the Internet for privacy violations. Indeed, the very act of policing itself raises serious privacy concerns. ISPs do not control, nor have privity of contract, with the millions upon millions of websites, applications and services that run on their networks. The DMCA wisely protects user privacy and exempts service providers from having to monitor the contents of their users in order to be eligible for the DMCA's liability safe harbor.¹⁶ The third-party liability rules reflected in the DMCA and other laws such as the Communications Decency Act at Section 230,¹⁷ have promoted the widespread deployment of broadband and the associated products and services enjoyed by millions of users. To change that balance risks suppressing the development of new products and services yet to be conceived and offered to consumers.

report explained, "[T]he definition [of "initiate"] specifies that a company that merely engages in routine conveyance, such as an ISP that simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal, shall not be considered to have initiated the message." S. Rep. No. 108-102 (2003), at 15.

¹⁶ See 17 U.S.C. § 512(m).

¹⁷ See 47 U.S.C. § 230.

CONCLUSION

In a dynamic online environment with many different actors and situations, the current dialogue addressing online privacy issues is a healthy and important part of the ongoing evolution of broadband and online services. We believe that the focus should be on principles that both ensure a vibrant Internet that supports current and emerging content and services and also protects consumers in the use and collection of their personal information.

Respectfully submitted,

/s/ Neal M. Goldberg

Neal M. Goldberg
Loretta P. Polk
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

January 22, 2010