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

In the Matter of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Leslie Harris
David Sohn
John Morris
Greg Nojeim
Alissa Cooper
Heather West

Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, DC 20006
(202) 637-9800

June 8, 2009

Table of Contents

Summary

A national broadband plan should affirm and endorse the characteristics and policy choices that have been crucial to the Internet's success. Unlike other media platforms, the Internet gives users broad control over what they will see and hear. It can accommodate an essentially unlimited number of speakers. Its open technical standards enable widespread and unsupervised innovation. It is interoperable and global. It has no central gatekeepers controlling what or who gets on the network. To preserve these essential characteristics, a national broadband plan should embrace the key policies that have fostered them:

- Affording Internet communications the highest level of free speech protection;
- Avoiding government mandates dictating or interfering with technology design;
- Protecting intermediaries such as Web sites, Web hosting services, and Internet service providers against liability for content created by users; and
- Preventing discrimination by network operators against particular content, users, or devices.

A national broadband plan also should call for new policy initiatives to help spur the Internet's future growth. In particular:

- Stronger safeguards are needed to protect against discrimination that could undermine the Internet's openness. The plan should call for new legislation and the addition of a nondiscrimination principle to the Commission's broadband Policy Statement, among other steps.
- Stronger privacy standards, including national consumer privacy legislation, would help promote public confidence in the Internet as a platform for speech and commerce.
- The Electronic Communications Privacy Act should be updated so that Internet communications and "cloud computing" enjoy an appropriate legal framework concerning government surveillance.
- Federal agencies should proactively release more government data online, expand their use of interactive tools, and both stream and archive video of public government meetings.
- Efforts to protect children online should focus on educational initiatives and parental empowerment.
- Efforts to address copyright and cybersecurity protection must take care to treat online free expression, user empowerment, and privacy as core goals in developing policy.

Regarding scope and process, the Commission's plan should expressly target broadband used to provide *Internet service*. Other types of high-speed data transmission could be considered "broadband," but should not be the focus of the plan. Finally, the Commission should commit to publish and seek comment on a tentative version of a plan before it finalizes its report. Initial input on the wide-ranging questions set forth in the NOI is no substitute for input on actual elements of a proposed plan.

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

In the Matter of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commission's Notice of Inquiry ("NOI"), FCC 09-31, regarding the development of a national broadband plan for the United States. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet.

I. Introduction

The Internet today is a technology of freedom and innovation. In only about two decades, it has become a powerful, global platform for commerce, human development and democratic participation. While discussions of individual Internet policy issues sometimes focus on real or perceived threats or challenges that arise in the online world, the bigger picture is that the Internet offers overwhelming benefits. That is why Congress has established that "[i]t is the policy of the United States to promote the continued development of the Internet and other interactive computer services and other interactive media."[1] In the legislation that triggered the current proceeding, Congress has gone one step further and declared that the nation needs a plan "to ensure that all people of the United States have access to broadband capability."[2] The legislation also provides funds to support broadband infrastructure deployment.

"Broadband" is not necessarily entirely synonymous with "Internet." Broadband technology, in the generic sense of high-capacity data transmission capability, could be used to provide connectivity within more limited networks or for more limited purposes. But it is broadband's ability to connect users to the full Internet, with all its myriad and evolving uses, that justifies developing a national plan.

While it is important to consider mechanisms for directly encouraging the build out of broadband's physical infrastructure, therefore, it is equally important to ensure that the United States maintains and indeed strengthens the legal and policy framework that has enabled the Internet to become such a dynamic and innovative medium. The

[1] 47 U.S.C. § 230(b)(1).
[2] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) ("Recovery Act") § 6001(k)(1).

characteristics that have been key to the Internet's rapid growth to date will also be essential components of any strategy to bring broadband to "all people of the United States" – because these characteristics are what will enable the Internet to support the ever changing array of uses that will attract new users and fuel ongoing growth. These characteristics are also what will make the government's efforts in this area worthwhile. After all, even if government could find a way to ensure access to a more static or constrained broadband network for all or most Americans, the benefits of doing so would be radically diminished.

These comments will focus on policies to preserve and promote the characteristics that make the Internet so successful. The first section will review the legal and policy choices that have enabled the Internet to thrive. These choices should not be taken for granted; they frequently are subject to debate and pressure from competing policy objectives. It therefore is essential that a national broadband plan recognize and endorse the policy foundations on which the Internet's success rests. The second section of these comments will then turn to a number of areas in which the plan should include reforms, legislation, or new initiatives to spur Internet usage and deliver the benefits envisioned by Congress in the Recovery Act. Finally, the third section will suggest that this proceeding should focus on broadband used to deliver *Internet* service and should include an opportunity for public comment on an actual tentative plan at some point before the plan is finalized.

One area these comments will not address is how broadband stimulus funds or other government subsidies or programs may directly facilitate the deployment of broadband infrastructure. CDT recognizes that such policies carry significant benefits and should constitute a significant part of a national broadband plan. The focus of these comments, however, is the suite of policies that must be coupled with deployment measures in order for a broadband plan to be fully successful.

II. Affirming the Policy Framework Behind the Internet's Growth

A. How the Internet Differs from Other Media

A national broadband plan should reflect a clear understanding and appreciation for the characteristics that make the Internet different from other media platforms. In particular, a plan should place high priority on ensuring that the following elements are maintained and indeed strengthened.

User control: The Internet is uniquely user-controlled. To a far greater extent than users of any other electronic medium, Internet users have the power to choose where they will go online and what they will see and hear. Users can configure their Web browsers and their search engines to avoid content they consider objectionable. They can install filters to block unwanted content and email. Assuming users are provided with notice and genuine choices, they can decide what software to download. They can install security software to protect against many forms of fraudulent behavior.

Abundance and low barriers to entry: Traditional radio and television technology was

bound by a limited technical capacity to exploit the electromagnetic spectrum. Consequently, regulation of the airwaves was deemed necessary in order to allocate what was seen as a scarce resource. The Internet, by contrast, can accommodate an essentially unlimited number of points of entry and an essentially unlimited number of speakers. Its open platform accommodates many-to-many, one-to-many, and one-to-one communication. Compared to the cost of a printing press, a television station, or a radio tower, the cost of launching a Web site is remarkably low – and that Web site can reach the entire world.

Very low barriers to entry and participation have led to relative equality of voice – a democratization of expression. In terms of free speech, an environmental activist can reach the same number of people as an oil company. A blogger can impact an election as much as a major newspaper. And a new content or application provider can emerge from nowhere to become an extraordinary success with relatively low investment and without having to obtain a government license or negotiate with an incumbent before rolling out new services.

Openness to innovation: The Internet supports a remarkable degree of innovation. It does so on the basis of voluntary technical standards. Even though the Internet was "born" under the auspices of the Pentagon, the U.S. Government never mandated its core technologies. Rather, the key technologies, such as the TCP/IP suite of protocols, were developed by engineers and adopted broadly because they worked. The open nature of those standards enables anyone to design products and services that make use of the shared protocols. No permission or pre-approval is required; all it takes is adherence to the protocols. In short, the standards-based nature of the Internet creates a remarkably rich and open platform for innovators of all kinds. The openness of the platform has enabled individuals, tiny startups, and noncommercial collaborators to pioneer such groundbreaking innovations as the World Wide Web, instant messaging, Google, social networking, and Wikipedia.

Interoperability and global reach: The brilliance of the TCP/IP suite of protocols is that it enables any device attached to the edges of the network to interoperate with other devices at the far reaches of the network. Geography matters little; an Internet user with a message or an innovation to share can reach the whole world. The Internet is interoperable and global.

No gatekeepers, decentralization: Essential to each of the characteristics listed above is the Internet's decentralized structure and lack of gatekeepers. Unlike previous mass media, the Internet was designed to be decentralized, with most power at the edges of the network (the users and their devices) and very little "intelligence" or functionality in the center (the transmission network that carries communications between users). This architecture makes it difficult to exercise centralized control or supervision. Above all, it means the network lacks any central gatekeepers. The absence of gatekeepers is what enables the medium's user control, low barriers to entry, and openness to innovation. Internet users can communicate and innovate in evolving and unforeseen ways without needing to navigate any licensing, regulatory, or approval process. It would be a very

different Internet today if the permission or consent of gatekeepers – governments, network operators, or anyone else – were a prerequisite for effective use of the medium.

B. Legal and Policy Foundations of the Internet's Success

The characteristics that distinguish the Internet did not arise in a legal vacuum. From the outset, the Internet's growth has been facilitated by a lightweight policy framework that suited and supported its unique technical architecture. Unfortunately, debates over objectionable content online, protecting intellectual property, preventing terrorism or restructuring telecommunications policy sometimes seem to lose sight of what makes the Internet special. The result can be heavy-handed policy proposals that could place the Internet's core characteristics at risk.

A national broadband plan should expressly embrace the legal and policy framework that has fostered the Internet's growth. Doing so is essential to achieving the Recovery Act's goals of "maximum utilization of broadband infrastructure and service by the public" and advancing consumer welfare and the other policy objectives cited in the statute.[3] Specifically, the plan should strongly and clearly endorse the following policies.

Highest level of free speech protection: The Supreme Court ruled early on that the Internet was entitled to the strongest form of First Amendment free speech protection, and that conclusion has been repeatedly reaffirmed over the past 13 years.[4] Critical to the courts' protection of Internet speech are the differences from traditional media listed above – particularly user control, abundance, and low barriers to entry. For example, regulation in the broadcast context historically has been justified by the scarcity of the medium (the number of possible speakers is limited) and the idea that broadcasting content comes essentially unbidden into any home tuned to a particular channel. In contrast, there is no scarcity regarding who can speak over the Internet or how much they can say; Internet content is delivered only to users who choose it; and, critically, parents are able to use software and other technology tools to protect their children from unwanted content. Based on such factors, court have found that historical justifications for content regulation are wholly inapplicable to the Internet. This Internet jurisprudence has prevented government-based gatekeeping in the form of censorship, preserved the principle of user control, and enabled the development of robust new forums for speech such as video sharing Web sites and social networking.

Avoiding technology mandates: From the outset, Internet policy was based on the notion that government should not dictate or interfere with the design of technology. For example, early efforts to control encryption were abandoned in part based on the recognition that government-mandated back doors would undermine security rather than improve it. Government technology mandates raise entry barriers and hinder innovation. Given the Internet's global nature, technology mandates or other burdensome regulation

---

[3] Recovery Act § 6001(k)(2)(B), (D).

[4] *See, e.g., Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997); *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004); *American Civil Liberties Union v. Mukasey*, 534 F.3d 181 (3rd Cir. 2008).

of technology in the United States could simply send innovation overseas.

Safe harbors for Internet intermediaries: Congress expressly decided that intermediaries such as Web sites, Web hosting services, and Internet service providers ("ISPs") should not be liable for content created by their users. In section 230 of the Communications Act and section 512 of the Digital Millennium Copyright Act, Congress provided important safe harbors from liability in such areas as defamation and copyright.[5] These protections from liability are what have enabled interactive and "user-generated content" sites to flourish. If ISPs, Web hosts, and Web sites with no bad intent were instead made potentially liable for content posted by others, they would have no choice but to assume new gatekeeper roles and pare back on functions that empower communication by and among users. Entry barriers for new Internet services (and new competitors to existing services) would increase substantially, the platform's openness to innovation would be reduced, and service providers would be reluctant to host controversial but lawful speech.

Nondiscrimination by network operators: The early Internet piggybacked on the telephone network, the operators of which were required to carry all traffic on a nondiscriminatory basis and to allow attachment of any equipment that did not harm the network. Therefore, innovators did not need to negotiate with network operators to connect a modem to the network or to make their content or services available to a wide audience. More recently, the Commission's 2005 broadband Policy Statement established that users should be able to access any Internet content and services of their choice, without interference from their broadband provider.[6] The Commission's ruling against Comcast in 2008 established that network operators must not pick out certain applications and degrade the associated traffic.[7] Such discrimination could, as a practical matter, turn the network operator into a gatekeeper whose permission is needed in order to avoid degraded transmissions. The result would be less user control and less openness to innovation.

A national broadband plan should expressly affirm that each of these elements – strong First Amendment protection, avoidance of technology mandates, liability protections for Internet intermediaries, and nondiscrimination by network operators – are core policies that must be vigorously maintained. Firm resistance to efforts to weaken or depart from these policies should be an explicit part of the plan.

III. New Policies and Initiatives To Spur the Internet's Continued Development

In addition to reaffirming the government's commitment to the core policy framework that has helped support the Internet to date, a national broadband plan should call for a

[5] 47 U.S.C. § 230(c)(1); 17 U.S.C. § 512.

[6] *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Policy Statement, 20 FCC Rcd 14986 (2005) ("Policy Statement").

[7] *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, Memorandum Opinion and Order, 23 FCC Rcd 13028 (2008) ("Comcast Order").

number of policy initiatives and reforms that could help spur the Internet's continued growth. Many of these steps would serve important policy aims that arguably may be outside the scope of a broadband plan. For example, protecting privacy is a valuable goal in its own right. So is increasing the accessibility of government to its citizens. But each also will help foster growing broadband usage and demand, by encouraging more citizens to take advantage of the benefits that broadband Internet can deliver. They therefore can help to achieve "maximum utilization of broadband" and advance consumer welfare and the other goals cited in the Recovery Act. While many of these policies are outside the Commission's normal jurisdiction and would need to be implemented by Congress or other entities, a broadband plan could well recommend action on these fronts.

A. Strengthen Safeguards Against Harmful Discrimination by Broadband Operators

As discussed above, broadband Internet providers have not exercised centralized control over what applications, services, or content are allowed or how they must be designed. This is a big part of what has made the Internet such a fertile ground for innovation. But the future of this "neutral" architecture is not guaranteed. Broadband providers could seek, for example, to prioritize selected traffic or to impose limits on traffic associated with certain high-bandwidth applications. In addition, an increasing number of users are connecting to the Internet via wireless networks, which traditionally have been subject to a greater level of central control than the wireline Internet.

Regulatory safeguards are needed to protect against the risk that broadband providers, by favoring some Internet traffic over others, could exert creeping gatekeeper control and undermine the medium's openness to independent innovation.

At the same time, extensive or burdensome regulation is clearly not desirable. Overbroad rules could interfere with legitimate network management or slow the pace of innovation by subjecting a broad range of Internet-related activity to new regulatory supervision. Indeed, a bright line needs to be drawn between enacting regulatory safeguards aimed at preserving Internet neutrality and assigning regulatory responsibility for Internet matters generally. While the former is desirable, the latter would carry long term risks to the Internet's minimally regulated environment, regardless of the agency chosen.

At present, the principal regulatory protection for the continued openness of the Internet is the Commission's stated commitment to enforce its 2005 Policy Statement. That commitment, however, remains subject to the cloud of pending litigation over the lawfulness of the Commission's 2008 Comcast Order. Just as important, the broadband principles set forth in the Policy Statement guarantee "access" to Internet content and services but do not say anything about the quality, speed, or reliability of a user's access to his or her chosen content and services. In short, they do not on their face address discrimination that falls short of full blocking of access.

A national broadband plan should include several provisions to protect against discriminatory treatment that could undermine the Internet's openness and give

broadband operators an increasing degree of gatekeeper control.

Legislation: A national broadband plan should call for legislation expressly authorizing the Commission to police and prevent discriminatory behavior by network operators that could undermine the openness of the Internet. The goal would be to both codify and cabin the Commission's role in this area, and to provide statutory guidance concerning what kinds of discriminatory practices will be treated as unlawful. Such legislation is needed because, while the Commission's Comcast Order rightly recognized that Comcast's practice of singling out a specific protocol for inferior treatment represented a major and harmful departure from the Internet's neutral architecture, the decision also asserted a dangerously elastic concept of Commission regulatory authority over Internet matters.[8] The Commission role in this area should be authorized and delineated by statute, not open-ended.

Adding nondiscrimination to the Policy Statement: As noted above, the principles set forth in the Commission's Policy Statement, on their face, say that users are entitled to access whatever they choose on the Internet but say nothing about the quality, speed, or reliability of that access. Degrading traffic, however, can serve largely the same ends as blocking access, if it impairs the performance of a particular product, service, or application to the point that users start deserting it (or, in the case of a new service, never adopt it in the first place). Like outright blocking, degradation can permit the network operator's decisions, rather than the preferences of users, to determine what online services and applications will succeed.

In connection with a national broadband plan, therefore, the Commission should modify its Policy Statement to expressly address discrimination that falls short of outright blocking. A nondiscrimination principle would, like the rest of the Policy Statement, be subject to the "reasonable network management" exception. Such a principle could, for example, take the following form:

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to access and use the content, applications, service, and devices of their choice without unreasonable discrimination by their network provider with respect to speed, service quality or price.

Making nondiscrimination a prerequisite for federal support: Recovery Act states that recipients of broadband stimulus money will be subject to interconnection and nondiscrimination requirements. A national broadband plan should call for such

[8] The Comcast Order stated (¶ 15) that the Commission's action was ancillary to (among other provisions) section 230(b) of the Communications Act, which cites such broad policy goals as "promoting the continued development of the Internet and other . . . interactive media." This rationale would appear to open the door to virtually any regulatory action that the Commission might in the future come to view as "good for the Internet." Indeed, it could even be misused to try to justify regulatory action aimed at entities providing online content rather than network connectivity, since fighting objectionable content could be deemed a core purpose of section 230.

requirements to be included in all future broadband deployment assistance programs as well. The basic policy principle is simple: federal funds should not be used to subsidize broadband infrastructure that is anything less than fully open and flexible. Grantees should not be permitted to narrow user choices or pick winners and losers on infrastructure partly or fully supported with public money.[9]

Creating a preference in federal programs for wholesale (open access) providers: A national broadband plan could promote competition and consumer choice by directing that federal broadband assistance programs give a preference to applicants that commit to operate broadband facilities on a wholesale basis. Such applicants would agree to allow their infrastructure to be used by independent third parties for the provision of retail broadband services to end users. (Applicants might also offer retail services of their own over the same facilities.) Congress embraced such a model in the Recovery Act's provisions for the RUS broadband program: "priority for awarding such funds shall be given to project applications for broadband systems that will deliver end users a choice of more than one service provider."[10] Particularly in areas where broadband deployment is just starting and the market may not easily support multiple infrastructures, wholesale services may offer the best opportunity for achieving competition in consumer broadband offerings.

Developing best practices for network management: "Network management" generally refers to technical actions that network operators take to keep the network running efficiently and avoid problems. Sometimes these actions require operators to differentiate among Internet traffic. Therefore, safeguards against discrimination may need to make allowances for reasonable network management, as the Commission's Policy Statement does. Network management must not, however, be permitted to serve as an excuse or loophole for practices that enable network operators to pick winners and losers or to assume effective gatekeeper control.

A national broadband plan could address the question of network management by calling on network operators to develop a set of best practices or guiding principles regarding acceptable network management techniques. The plan should call for norm setting in this area to distinguish between two very different categories of network management. Techniques to mitigate the impact of sporadic network congestion could be termed "congestion management." Techniques used by network operators to protect against or block Internet communications that are illegal, harmful to the network, or harmful and/or unwanted from the perspective of users could be termed "security management." The two may require different sets of best practice principles.

For congestion management in particular – the kind of network management at issue in the Comcast Order – the broadband plan should express some basic expectations. Specifically, the goal of best practices efforts in this area should be to ensure that

---

[9] CDT's views concerning the definition of the Recovery Act's interconnection and nondiscrimination obligations are set forth in its April 13, 2009 comments to NTIA, available at http://www.cdt.org/speech/net-neutrality/20090413_NTIA_comments.pdf.

[10] Recovery Act, Division A, Title I.

carriers' network management practices are:

- applied fairly and evenly, using objective criteria such as volume of bandwidth usage;
- consistent with the common networking standards on which the Internet is based; and
- sufficiently transparent to both consumers and developers of Internet applications.[11]

Best practices should not aim to dictate implementation details or preclude experimentation, but rather to ensure that network operators steer clear of tactics that would violate these principles.

Extending policies to wireless: The importance and prevalence of wireless Internet access is only likely to grow. As more and more Internet users rely on wireless connections, it will be essential to ensure that the characteristics and policies that have supported the success of the wireline Internet are carried forward. Broadband use would suffer if the move to a more mobile Internet were to come at the expense of the medium's openness. A national broadband plan therefore should include a commitment to ensure that safeguards such as the Commission's Policy Statement are extended to Internet access delivered over wireless broadband.

B. Enact National Consumer Privacy Legislation and Promote Strong Privacy Standards

The Commission's NOI asks generally about consumers' privacy expectations when using broadband, how privacy enhances consumer welfare, and whether privacy protections can be achieved through self-regulation or will require some kind of congressional or agency action. The NOI also seeks guidance on the specific practices of behavioral advertising and deep packet inspection.[12]

Privacy is an essential building block of trust in the digital age. Privacy protections help to secure our communications and sensitive data, providing a foundation for e-commerce and the full realization of the potential benefits of the networked world. Privacy and the ability to remain anonymous are also fundamental to free expression, which has flourished nowhere more vibrantly than on the broadband Internet. For the broadband Internet to continue to thrive, consumers need to be assured that their communications and transactions will be as secure, confidential, and anonymous as they desire.

In recent years, however, and at an accelerating pace, technology and market forces have created fundamental challenges to online privacy. More data is collected about individuals and retained for longer periods than ever before. Massive increases in data storage and processing power have sown the seeds for diverse new business models predicated on the collection, analysis and retention of richly detailed data about

---

[11] CDT has advocated these guiding principles for network management in prior comments to the Commission, available at http://www.cdt.org/speech/20080213_FCC_comments.pdf and http://www.cdt.org/speech/20080228_FCC_comments.pdf.

[12] NOI ¶¶ 58-60.

consumers and their online activities. Study after study has shown that consumers do not understand how their data is used under these new models – and when they find out, it is cause for great concern.[13] Privacy worries continue to inhibit some consumers from engaging in even more established business models such as online shopping.[14]

A national broadband plan should reinforce privacy's crucial role in building consumer trust in the Internet. The plan should include a number of different components in this vein, the most pressing of which is support for a federal consumer privacy law.

***Enacting a federal privacy law*:** Despite how critical privacy protections are to the continued health of the Internet, the United States lacks a comprehensive consumer privacy law. Instead, American consumers currently face a confusing patchwork of privacy standards that offer only weak protections for much personal information collected by businesses and that leave some information unprotected in surprising ways. For example, while there is a strong privacy law for cable viewing records,[15] no law protects online purchasing data, and while the Commission's CPNI rules offer protections for location information collected by carriers,[16] no comparable rules exist for the same information collected by other service providers.

To close these gaps, the national broadband plan should call on Congress to enact general privacy legislation. Simple, flexible legislation would protect consumers from inappropriate collection and misuse of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of Fair Information Practices,[17] including requiring transparency and notice of data collection practices, minimizing data collection and retention, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.

Such a comprehensive privacy framework can only conceivably come from Congress. While the Commission may believe it would have authority to address certain

---

[13] *See, e.g.*, Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings,* Mar. 2008 (in which the majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, *Use of Cloud Computing Services*, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf, Sept. 2008 (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[14] *See* John B. Horrigan, *Online Shopping*, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf, Feb. 2008.

[15] *See* 47 U.S.C. § 551.

[16] 47 C.F.R. § 64.2001 et seq.; see also 47 U.S.C. § 222.

[17] The Fair Information Practices are a widely recognized set of principles that provide the basis for information privacy protection. *See, e.g.*, Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, Sept. 1980.

components of such a framework pursuant to ancillary jurisdiction, having the Commission delve into privacy in this piecemeal fashion would only further complicate the jumbled patchwork of privacy regulations that exist today. The goal should be to create a uniform set of protections for personal data collected both online and offline, regardless of the communications medium or service with which it associated. Congress is best positioned to develop such a framework. Moreover, primary responsibility for agency-level leadership and enforcement on privacy matters should remain with the Federal Trade Commission, as it has the most relevant experience in the area.

While self-regulation would likely still be necessary to address certain areas not covered by a baseline privacy law, it cannot suffice on its own. The online advertising industry provides a useful demonstration of how self-regulation comes up short: after nearly a decade under a self-regulatory framework that has routinely been criticized as inadequate,[18] the industry has only just begun to make improvements in response to intense pressure from the FTC,[19] and even those changes have yet to meet the self-regulatory standards proposed by the agency.[20] Protecting personal data across the board will require a rigorous mix of self-regulation, enforcement of existing law, and a new general privacy law backed up by regulatory enforcement.

Addressing DPI: Deep packet inspection ("DPI") is among the many areas in which a baseline privacy law could provide important clarification for consumers and businesses alike. In part because the Internet was developed based on a decentralized architecture and the "end-to-end principle," consumers have come to expect that their Internet communications pass through the network without being snooped on along the way. DPI dramatically alters this landscape by providing an ISP with the ability to inspect consumer communications en route. Thus, DPI defies the expectations that consumers have built up over time about how their broadband Internet service works. Absent unmistakable notice, consumers simply do not expect their ISP to be looking into the content of their Internet communications.

DPI poses unique risks to individual privacy.[21] DPI technologies potentially allow ISPs and other intermediaries to analyze all of the Internet traffic of millions of users simultaneously – without any indication to end users. In many cases, DPI equipment will automatically collect personally identifiable information (PII) or sensitive data (such as

---

[18] *See* Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and Self-Regulation*, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf, Nov. 2007.
[19] Network Advertising Initiative, *2008 NAI Principles*, http://networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf, Dec. 2008.
[20] Federal Trade Commission Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, http://www2.ftc.gov/opa/2009/02/behavad.shtm, Feb. 2009; Center for Democracy & technology, *Response to the 2008 NAI Principles: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising*, http://www.cdt.org/privacy/20081216_NAIresponse.pdf, Dec. 2008.
[21] For an extensive discussion of the privacy risks of DPI, see Leslie Harris, *Statement of Leslie Harris before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet: "The Privacy Implications of Deep Packet Inspection,"* Apr. 23, 2009, http://www.cdt.org/privacy/20090423_dpi_testimony.pdf.

personal health information), even if the ISP has no intention of using such data. And as DPI technology matures, it is likely to become an increasingly attractive tool for government surveillance, given that the government in recent years has shown a large appetite for electronic data gathering.

Certain uses of DPI may already be regulated or prohibited under the federal Wiretap Act and the Cable Act. For example, some uses of DPI to compile behavioral advertising profiles would probably run afoul of both statutes absent unavoidable notice and opt-in consent.[22] However, the boundaries of both laws are not clear in all contexts. Moreover, the Wiretap Act was last modified more than 20 years ago and has not kept pace with technology, and the Cable Act applies only to cable providers. These laws simply do not provide sufficient protection to consumers against DPI's risks.

Privacy legislation could help address the privacy challenges posed by DPI. In addition, the national broadband plan should call on Congress to examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. The Electronic Communications Privacy Act (which amended the Wiretap Act) was passed more than 20 years ago, long before there was a World Wide Web and the Internet became integrated into Americans' daily lives. The application of the law to both common online activities and services making use of emerging technologies like DPI remains unclear and the legal protections it provides for the enormous amounts of personal data stored online are far too low. As discussed below, updating this law should be a core component of the national broadband plan.

Addressing location privacy: The ubiquity of increasingly high-powered mobile devices has already spawned the Internet's first generation of location-based services and applications. As the accuracy of location data improves and the expense of calculating and obtaining it declines, location awareness may well come to pervade the online experience. While the increasing availability of location information paves the way for exciting new applications and services, the increasingly easy availability of location information raises several different kinds of privacy concerns.

Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may potentially describe both what a person is doing and where he or she is doing it. The ubiquity of location information may also increase the risks of stalking and domestic violence if perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims.

Furthermore, location information is and will continue to be of particular interest to government and law enforcement. Standards for government access to location

---

[22] *See An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising*, Appendix A to the Statement of Alissa Cooper Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110th Cong. (2008) http://cdt.org/testimony/20080717cooper.pdf.

information held by companies are unclear at best and far too low at worst.[23] The existence of detailed records of individuals' movements should not automatically facilitate the ability for governments to track their citizens, but in many cases, laws dictating what government agents must do to obtain location data have not kept pace with the evolving technology.

Ideally, national privacy legislation would address the risks raised by increased availability of location information by including (among other Fair Information Practice protections) a provision requiring that the disclosure of precise location information in a commercial context be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties. In addition, the broadband plan should suggest that any update to ECPA, discussed further below, should amend the standards for government and law enforcement access to location information to make clear that a probable cause warrant is required for the government to obtain location information.

Exercising active FTC oversight and leadership: A national broadband plan should call on the FTC to continue to play an active role in promoting strong privacy practices, even in advance of the enactment of any further legislation. For example, with respect to the NOI's questions about behavioral advertising,[24] the FTC earlier this year released self-regulatory guidelines for online behavioral advertising that create a high standard for privacy.[25] There is currently no formal way to evaluate how the online advertising industry's practices are living up to those principles, however, so ongoing FTC oversight is essential. In addition, data collection for behavioral advertising often provides consumers with an ability to opt out, but it has been known for years that the mechanisms for exercising that choice are technically inadequate and difficult to use. A broadband plan should call on the FTC to work with industry to explore ideas for improving consumer choice online, including the possibility of a "Do Not Track List," a proposal submitted to the FTC by a group of public interest advocates in 2007.[26]

C. Reform the Electronic Communications Privacy Act (ECPA)

Consumer privacy concerns encompass not only what companies do with their data, but also the extent to which the government accesses it. Failure to ensure that statutory

---

[23] *See* Center for Democracy & Technology, "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology" (2006), available at http://www.cdt.org/publications/digital-search-and-seizure.pdf. Over the past few years courts have split on the standards protecting location information, with a majority of courts rejecting governmental arguments for a low standard. *See, e.g., In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 07-524M (W.D. Pa. Sept. 10, 2008), (available at http://www.eff.org/files/filenode/celltracking/lenihanorder.pdf). CDT joined an amicus brief that details the key legal argument for a strong standards, available at http://www.cdt.org/security/20080731_lenihan_amicus.pdf.

[24] NOI ¶ 59 & fn. 86.

[25] Federal Trade Commission Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, http://www2.ftc.gov/opa/2009/02/behavad.shtm, Feb. 2009

[26] Pam Dixon et al, *Consumer Rights and Protections in the Behavioral Advertising Sector*, http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf, Oct. 2007.

privacy protections vis-à-vis government surveillance keep pace with technology degrades the effectiveness of those protections, increases the consumer concern about conducting on-line activity, and could undermine benefits that an effective broadband policy would otherwise impart. Consumers will not embrace broadband if they have a sense that everything they do online will be watched by government officials.

The law that protects consumers against such surveillance, the Electronic Communications Privacy Act of 1986 ("ECPA"),[27] is badly out of date. To take but one example, ECPA was enacted long before "cloud computing" became the growth industry that it is today. Personal calendars, family photos and sensitive business documents that used to enjoy a high level of legal protection when locked away in desk drawers or on password-protected computers are now held by third party service providers in the Internet "cloud" – where, under ECPA, they currently enjoy only minimal protection against government snooping. A strong broadband plan should work to foster the growth of cloud computing and all of the efficiencies it promises. But the minimal protection that is afforded cloud computing information could hold back that growth as consumers and businesses come to recognize this privacy deficit. As discussed above, ECPA also fails to provide clarity concerning government access to data gathered via DPI and to location privacy information. The broadband plan should include a recommendation that ECPA be updated to keep pace with technology.

ECPA reform recommendations should also specifically reject data retention mandates that would undermine consumer confidence in the privacy of their online activities. For example, a mandate requiring ISPs, Web site operators, wireless carriers, employers who provide employees with Internet access, hotels, libraries, and universities to maintain for an extended period of time data identifying their customers' online activity just in case law enforcement officials some day sought the data would threaten privacy and pose a security risk. A mandate of this kind would result in collection of large amounts of information that could be abused, mistakenly disclosed, or hacked into for fraudulent and other illicit purposes. To the extent that such mandates make consumers or businesses distrustful of the privacy of their online transactions and communications and depress Internet use, data retention mandates could undermine the promise of an effective broadband policy.

D. Use Broadband To Promote Transparency and Citizen Interaction in Government

The NOI asks how public awareness and participation in government can be amplified by access to broadband; how new media tools can advance civic participation; and about the benefits of video streaming of government meetings.[28] As these questions suggest, broadband has great potential to facilitate public access to information about government and to resources that enable more interactive citizen participation in government decision-making. But deployment of broadband will not deliver these benefits automatically; government entities must pitch in by taking the necessary steps to

[27] 18 U.S.C. § 2510.
[28] NOI ¶¶ 70-71.

embrace the new capabilities that the technology offers. To achieve the Recovery Act's objective of "advancing . . .civic participation,"[29] the national broadband plan should call for such measures as the proactive online release of government data, the expanded use of interactive tools in government, and widespread Web streaming of video of public government meetings.

Enabling online access to government data: The Federal Government collects, processes, and acts on a tremendous amount of data. Broadband service creates the potential for easy public access to this large body of information. However, much of this information is currently not accessible online, meaning that as a practical matter it is readily available only to a small subset of the country, if at all. All public government data should proactively be placed online. Accessibility could be maximized by using open data formats and creating effective public Web sites to explain the information in context. These goals should be stressed at all federal agencies.

Tasking CIO Offices with Responsibility for Disseminating Information: Each agency's Chief Information Officer ("CIO") should create a position focused on taking charge of data dissemination and transparency efforts for that agency. Working with the CIO, this official should have authority to review programs and system acquisitions, as well as to determine overall strategy concerning what and how information held by the agency should be made public online.

In addition, the CIO Council should develop recommendations for information dissemination initiatives and facilitate coordination and collaboration among agencies.[30] One task that would benefit from near-term CIO Council guidance is the creation of an index for the information held by each agency, using the Government Information Locator Service ("GILS"),[31] which would then be placed on both the agency's own Web site and on data.gov. Such an index, once compiled, would be an important reference point for each agency as it works to determine what information it should be making available online.

Using Innovative Tools to Spur Participation: One result of broadband access has been the increase in use of interactive social media and networking tools. While government has not yet begun to use these tools extensively, they could serve as a major avenue for civic participation if implemented correctly.

Video Streaming of Public Government Meetings: A national broadband plan should call for agencies all across government to stream video of public meetings and archive meeting video online. There are hundreds of federal boards, councils,

---

[29] Recovery Act § 6001(k)(2)(D).

[30] The CIO Council was codified by the E-Government Act of 2002. *See* 44 U.S.C. § 3603. Information about the CIO Council can be found at http://www.cio.gov/.

[31] GILS is an effort to use a common set of technical standards to identify, locate, and describe publicly available Federal information resources, including electronic information resources. *See* http://www.gpoaccess.gov/gils/index.html.

commissions, and committees that hold public meetings, but these meetings are typically limited to attendees that can physically attend. Streaming video of the meetings online would allow anyone with broadband access to watch or participate in the meeting. In addition, archived meeting video would allow citizens to catch up on public meetings after the fact, or refer back to the meeting before a transcript can be created. These video streams could be integrated with other tools to accept public comments during and after the meeting broadcast.

Funding transparency and open government efforts: All branches of the government need proper funding and resources dedicated to transparency efforts in order to achieve a systematic expansion of online information dissemination. Recent years have seen improvements in FOIA policy but little direct help in terms of resources for agencies struggling to properly implement the law. In addition, government bodies often are not well funded in terms of technical resources to do video streaming, adopt the latest Web site techniques, or otherwise facilitate transparency. A national broadband plan should call for appropriate funding and resources to enable the government to disseminate information in the most effective ways and to empower civic participation online.

E. Promote Education and Parental Empowerment as the Best Means for Protecting Children Online

For the past ten years, numerous blue ribbon panels have concluded that education and parental empowerment are the best and most effective approaches to concerns about online safety. In the early 2000s, an authoritative committee led by former Attorney General Richard Thornburg issued a National Research Council report entitled "Youth, Pornography and the Internet," concluding that education would be more effective than regulation.[32] This report echoed the early findings of the Final Report of the COPA Commission.[33] Most recently, the Harvard-run Internet Safety Technical Task Force released, in January 2009, a comprehensive report on online safety, concluding that education was vital.[34]

Congress has already taken action to promote education. In October 2008, Congress enacted the Broadband Data Improvement Act, directing (among other actions) the Federal Trade Commission to launch an online safety educational effort.[35] And last week, under the auspices of the Department of Commerce, the Congressionally-created Online Safety and Technical Working Group ("OSTWG") met for the first time.[36] OSTWG is dedicating a significant amount of attention to the question of online safety

---

[32] Nat'l Research Council of the Nat'l Academy of Sciences, *Youth, Pornography, and the Internet* (2002), available at http://books.nap.edu/html/youth_internet/.
[33] COPA Commission, *Final Report* (2000), available at http://www.copacommission.org/report/.
[34] *Enhancing Child Safety and Online Technologies, Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (Dec. 31, 2008), available at http://cyber.law.harvard.edu/research/isttf.
[35] Broadband Data Improvement Act, Pub. L. No. 110–385, 122 Stat. 4096 (2008) sec. 212.
[36] For information about OSTWG, see http://www.ntia.doc.gov/advisory/onlinesafety/index.html.

education.

A national broadband plan should take these and other educational initiatives and make them high priorities for the Federal government. Just as there are risks to minors in the offline world, there are risks in the online environment, and young people today should be taught how to stay safe online. The Internet offers enormous benefits to young people, and we must not hamper access to those benefits because of fears about safety. Education – of both kids and parents – is the most effective way to address these concerns.

F. Adopt Online Free Expression and User Empowerment as Key Aspects of Copyright and Cybersecurity Policy

The NOI asks how copyright-related content protections and cybersecurity issues should factor into a national broadband plan.[37] Both copyright and cybersecurity are likely to be areas of considerable policy activity, as mass online infringement and online security threats are recognized problems that already have been targeted for high-level attention and leadership. Indeed, major copyright enforcement legislation was enacted in late 2008 to, among other things, create a new Intellectual Property Enforcement Coordinator in the White House.[38] On cybersecurity, the Obama Administration in May 2009 released the results of a comprehensive review of cybersecurity policy, calling for the appointment of a cybersecurity official in the White House and the development of a national cybersecurity strategy.[39]

A national broadband plan should endorse efforts to address challenges in both of these areas. It also, however, should clearly state that online free expression and user empowerment (including users' ability to maintain privacy) must be treated as core policy considerations in each area.

Copyright: A national broadband plan should establish the promotion of speech and creativity by individual Internet users as a significant goal of the nation's copyright policy going forward. Increasingly, broadband enables and encourages individuals to go beyond being passive recipients of commercially-produced media. Instead (or in addition), they blog, "tweet," post photos and videos, and so forth. The continuation of this trend is a big part of what will fuel broadband growth in the United States. Copyright policy, therefore, cannot focus solely on the issues and concerns facing large commercial copyright holders. Questions of copyright protection, fair use, orphan works, and others can affect an ever-broadening range of broadband users. A national broadband plan should call on copyright authorities, including the new I.P. Enforcement Coordinator, to place a high priority on adapting copyright policies to the new world of user-generated content and avoid steps that can create legal obstacles to individual

---

[37] NOI ¶¶ 55, 67, 73.

[38] Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-43, 122 Stat. 4256 (2008).

[39] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, at 7.

creativity.

Cybersecurity: The Obama Administration's recent Cyberspace Policy Review calls for a new cybersecurity coordinator in the White House and for an updated national cybersecurity strategy. In light of this, a national broadband plan need not revisit the questions such as what part of government should take the lead on cybersecurity nor seek to provide substantive answers to the security challenges that surely will be addressed in a cybersecurity strategy. Rather, the broadband plan should affirm the importance of the process that has already been launched for addressing cybersecurity threats.

In addition, a broadband strategy should state explicitly that for purposes of encouraging the beneficial use of broadband, measures to address cybersecurity must not be allowed to undermine the ability of ordinary broadband services to empower individual free expression, innovation, and privacy. The broadband plan should call on the White House cybersecurity official to recognize that the ability to communicate anonymously is important for free speech and must be maintained; that imposing specific security-based technology mandates on private sector entities can undermine broadband's flexibility and openness to innovation; and that information sharing to combat cybresecurity threats must respect users' legitimate privacy expectations.

IV. Definitions and Process

A. Definition of "Broadband"

"Broadband" in its most generic sense could be interpreted to refer simply to high speed data transmission capability. Thus, one could argue that a service dedicated to delivering high definition television or movies is a "broadband service." For purposes of a national plan, however, the Commission should focus directly on broadband service that provides access to the full Internet. It is only the capability to access the full richness of the Internet, with all its attendant benefits and uses, that justifies a national effort to promote broadband.

A definition of this Internet-focused conception of broadband would incorporate the following elements.

- The service supports and uses common and public transport and routing standards and protocols, including the Internet Protocol, to deliver communications over the Internet.
- The service is two-way; it enables users to both send and receive data over the Internet. Speeds need not be precisely symmetrical, but should be robust in the upstream as well as the downstream directions.
- The service can be used to send and receive data associated with the full range of content, applications, and services available on the Internet, as selected by the customer. This includes content, applications, and services offered by entities with *no affiliation or contractual relationship* with the user's broadband provider.

- The service should offer data transmission speed sufficient to support whatever types of applications have become common and customary for mainstream Internet users. This will of necessity be an evolving standard.

In many cases the same facilities are used to provide broadband services that meet the above definition and other services that do not. For example, it is common today for cable television providers to deliver Internet service and television service over the same set of facilities. There is no policy reason to discourage such shared infrastructure arrangements; indeed, revenues from non-broadband services may help defray the costs of infrastructure deployment and thus indirectly help support the broadband Internet service. The focus of the Commission's national broadband plan, however, should be promoting the accessibility and speed of the service providing broadband Internet access; other types of services should be addressed minimally if at all in the plan.

B. Process for Developing the National Plan

The Commission's NOI casts a wide net, asking numerous questions across a broad range of issue areas. This is entirely appropriate for the current stage of the policy development process.

Initial public input on the broad issues to be considered in the proceeding, however, is no substitute for more focused public input on the actual elements of an eventual draft plan. Comments at the front end of the process can be useful for ideas and general policy guidance, but simply cannot provide the same kind of detail and specificity that will be possible once the issues have been narrowed and the key proposals and questions identified with specificity.

As the process moves forward, therefore, the Commission should commit to publish and seek comment on a tentative version of a plan before it finalizes its report and recommendations. CDT recognizes that accommodating an additional round of public comment complicates the timing, because the Commission would need to have developed and written up its tentative proposals a few months in advance of the February deadline. But it is necessary in order to provide a meaningful opportunity for public feedback on specific proposals.

* * *

CDT believes that the elements addressed in these comments are necessary to establish the legal and policy framework that will best encourage the success and growth of the Internet as an open and innovative platform for economic growth, civic participation, and the other goals enumerated in the Recovery Act. They therefore should be included in the Commission's national broadband plan.

Respectfully submitted,

Leslie Harris
David Sohn
John Morris
Greg Nojeim
Alissa Cooper
Heather West

Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, DC 20006
(202) 637-9800

June 8, 2009