

principles should not bar efforts to manage congestion, but rather should require those efforts to be evenhanded. On the topic of online copyright infringement, the Commission should steer well clear of encouraging or pressuring ISPs to take on the fundamentally new role of actively inspecting and making legal judgments about users' communications. Finally, while self-regulation can help promote sound privacy practices that all parties seem to agree are important for building trust, self-regulation cannot be a complete answer and needs to be supplemented with legislation.

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

In our initial comments, CDT walks through the key ways that the Internet differs from other media and the legal and policy decisions that have fostered the Internet's unique characteristics.¹ In particular, we argue that a national broadband plan should expressly affirm that four key elements of the Internet's successful legal and policy framework – strong First Amendment protection, avoidance of technology mandates, liability protection for Internet intermediaries, and nondiscrimination by network operators – are core policies that must be vigorously maintained.

Of these four topics, nondiscrimination is a major focus of many other parties' comments, as discussed further below. In addition, some comments touch on the idea that U.S. policy regarding Internet matters has favored "light touch" regulation rather than detailed government mandates. First Amendment protection and liability protection for intermediaries, however, receive little attention. More broadly, few comments attempt a point-by-point review of the policy choices that have proved successful in empowering online innovation to date.

This may be because it is natural, in thinking about a national broadband plan for "our future," to focus on what *new* steps need to be taken. But it is vital to ensure that any national plan, as it builds new structures, also protects the foundation. Existing successful elements of the policy framework are not guaranteed and should not be taken for granted.

For example, the freewheeling nature of free speech online frequently prompts well-meaning but ill-advised efforts to rein in perceived threats. Congress enacted first the Communications Decency Act and then the Child Online Protection Act only to see them repeatedly struck down by the courts as unconstitutional, ultimately wasting 13 years and millions of dollars on attorneys and experts.² States have enacted numerous similar unconstitutional laws,³ and new legislative proposals that fail to take account of the First Amendment implications of their impact on online speech are all too common.

¹ Comments of the Center for Democracy & Technology ("CDT Comments") at 5-8.

² See Leslie Harris, *Internet Censorship: Dead or Just Dormant?*, Huffington Post (Feb. 2, 2009) (http://www.huffingtonpost.com/leslie-harris/internet-censorship-dead_b_163210.html) (briefly recapping history of CDA and COPA cases).

³ For a sample of state Internet regulation laws struck down as unconstitutional, see *PSINet v. Chapman*, 342 F.3d 227 (4th Cir. 2004) (Virginia statute); *Am. Booksellers*

Likewise, advocates and policymakers pursuing various legitimate policy goals – for example, protecting against copyright infringement, ensuring convenient intercept access for law enforcement, or promoting a robust 911 system – have often sought to impose technology design mandates or to hold Internet intermediaries broadly liable for the activities of users despite statutory safe harbors. For instance, bills periodically have been introduced in Congress to empower the Commission to impose broad mandates for content blocking or anti-copying technology.⁴ The United States Trade Representative is negotiating an intellectual property trade agreement that may address ISP liability and has been urged to include provisions requiring signatories to impose substantial responsibilities on ISPs to actively police their networks for illegal material.⁵ The South Carolina Attorney General has recently threatened a classified ad Web site with liability for traffic posted by users.⁶ And private lawsuits aiming to hold Internet intermediaries liable for user behavior remain common.

In short, crucial policy choices that have enabled the explosion of free speech and innovations such as social networking, user-generated content and online collaboration tools are not set in stone and indeed face competing pressures on a regular basis. A national broadband plan should include an explicit reminder and reaffirmation that the elements described in CDT’s comments remain foundational building blocks for a successful national broadband policy and must not be weakened or circumvented.

Found. v. Dean, 342 F.3d 96 (2d Cir. 2003) (Vermont statute); ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999) (New Mexico statute); ACLU v. Napolitano, Civ. No. 00-505 (D. Ariz., Aug. 11, 2004) (Arizona statute); Cyberspace Communications Inc. v. Engler, 142 F.Supp.2d 827 (E.D. Mich. 2001) (Michigan statute); American Libraries Ass’n v. Pataki, 969 F.Supp. 160 (S.D.N.Y. 1997) (New York statute).

⁴ See S. 2048, 107th Cong., 2nd Sess. (2002) (calling for the establishment of standard security technologies for use in any software or hardware that handles copyrighted media); S. 602, 110th Cong. 1st Sess. (2007) (as introduced) (authorizing Commission to require use of “advanced blocking technologies” for platforms that include the Internet); H.R. 5252, 109th Cong., 2nd Sess. (2006) (as reported in Senate) §§ 452-54 (calling for regulations on devices capable of handling digital broadcast television and digital broadcast audio content).

⁵ See Nate Anderson, *RIAA’s ACTA wishlist includes gutted DMCA, mandatory filters*, ars technica (Jun. 30, 2008) (<http://arstechnica.com/old/content/2008/06/inside-the-riaas-acta-wishlist.ars>).

⁶ See John Morris, *Grandstanding Against Craigslist and Threatening Free Speech to Boot* (May 15, 2009) (<http://blog.cdt.org/2009/05/15/grandstanding-against-craigslist-and-threatening-free-speech-too-boot/>).

B. CDT Responses to Selected Arguments

1. Arguments Concerning Nondiscrimination

A number of commenters, particular those associated with network operators, suggest that a broadband plan should not include any nondiscrimination requirements or policies beyond the Commission’s existing broadband Policy Statement.⁷

As a preliminary matter, arguments concerning the supposed threats of a nondiscrimination policy often seem to assume a very crude or extreme version of regulation. For example, AT&T warns at length about the dangers of carrying a nondiscrimination policy “to its logical conclusion” and “banning all differential treatment of packets,” going so far as to assert that a nondiscrimination policy would “mean the end of content-delivery networks like Akamai or Limelight.”⁸ But this is a straw man, put forward because it is easier to argue against than the kind of nondiscrimination policy that the nation might reasonably adopt. A sensible nondiscrimination policy, while protecting the Internet’s open nature, would provide leeway for differential treatment of traffic in appropriate circumstances. A national broadband plan should call for the crafting of reasonable nondiscrimination policies – not duck the crucial issue of discrimination simply because an overbroad version could be problematic.

In CDT’s view, a nondiscrimination policy – like the Commission’s Policy Statement – would allow for reasonable network management to protect against security threats. It would also allow for network management to address congestion, so long as the techniques used comply with several basic principles:⁹

- They should be applied fairly and evenly, using objective criteria such as volume of bandwidth usage – so that the network provider is not selecting which specific content or applications to favor or disfavor;
- They should be consistent with the common networking standards on which the Internet’s broad interoperability depends; and
- They should be sufficiently transparent to both consumers and developers of Internet applications.

In addition, a nondiscrimination policy should allow *consumer-controlled* differential treatment of Internet packets. Empowering consumers to designate particular applications or communications for higher or lower priority treatment is entirely different from having the network operator make that selection. When the network operator does

⁷ *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Policy Statement, 20 FCC Rcd 14986 (2005) (“Policy Statement”).

⁸ Comments of AT&T, Inc. (“AT&T Comments”) at 106.

⁹ See CDT Comments at 11-12. CDT suggests the terms “security management” and “congestion management” to differentiate between two different types of network management that may raise differing policy considerations.

not control which specific traffic gets favorable treatment, the risk of gatekeeper control recedes.¹⁰

Once one recognizes that a nondiscrimination policy would not ban all differential treatment of packets, many of the arguments offered by nondiscrimination opponents lose their force.

A frequent theme, for example, is that nondiscrimination or neutrality policies would undermine ISPs' flexibility¹¹ or inhibit their ability to innovate.¹² Sometimes these arguments even co-opt the rhetoric of openness, arguing that "networks should be open to collaborations."¹³

Certainly network operators need appropriate flexibility to figure out ways to better run the network. As noted above, nondiscrimination should not and need not interfere with that. But not all "flexibility" is consistent with the nation's broadband goals. Flexibility to abandon the concept of open, general-purpose Internet service in favor of a more supervised environment would be contrary to those goals. So would flexibility to devise "innovations" that, in the interest of helping an ISP capture more of the immense value that the network fosters, put the ISP in the position to exercise more centralized influence or control. Innovations at the network level that leave the platform more ISP-controlled and less open would risk undermining innovation at the edges. In short, network operator "flexibility" to choose to pare back the medium's future flexibility is *not* something a broadband plan should aim to protect. Nor is "openness" to new collaboration arrangements that would leave the platform less open to independent speakers and innovators.

Another argument is that the nation needs "smart pipes" rather than "dumb pipes."¹⁴ But value-laden terms like "smart" and "dumb" obscure rather than inform the debate. The real question is to what extent the "pipes" (i.e., the ISPs) should make judgments and decisions about what traffic is most important or most in need of special treatment – and to what extent those decisions instead could be left to end users. Clearly a strong case can be made for handling certain network management matters, like some security issues,

¹⁰ A network operator allowing users to prioritize traffic might need to provide some parameters or incentives to ensure that users do not simply mark all of their communications for priority treatment. A network operator might even establish some default settings. The key is that users should remain free to use their "priority bits" with whatever application they choose, including emerging or unusual applications that the network operator is not familiar with and hence would never have thought to prioritize.

¹¹ See, e.g., Comments of the U.S. Chamber of Commerce ("Chamber Comments") at 4; AT&T Comments at 113.

¹² See, e.g., Comments of the National Cable & Telecommunications Association ("NCTA Comments") at 39; Comments of Verizon and Verizon Wireless ("Verizon Comments") at 87-88.

¹³ Filing by Arts+Labs ("Arts+Labs Comments") at 7.

¹⁴ Chamber Comments at 5.

at the network level. On the other hand, a call for “smart pipes” can also be code for broader reliance on centralized evaluation and categorization of Internet communications. A broadband plan should recognize that for many purposes, a far better approach would be to put the network’s intelligence under control of *end users*, as suggested above. Indeed, a network that empowers *users* to determine the relative priority levels of traffic based on their individual needs would be far “smarter” than one in which the ISP makes broad across-the-board choices. Thus, a belief that networks could benefit from some built-in “intelligence” does not argue for giving ISPs broad discretion to discriminate.

Similarly, AT&T argues that the Internet Engineering Task Force’s approval of “Diffserv” shows that differential treatment of packets can be appropriate and compliant with Internet standards.¹⁵ CDT agrees with that basic point, as far as it goes. But Diffserv does nothing more than offer a sound and standards-based *technological method* for implementing differential treatment. Diffserv does not purport to address the crucial question of who chooses what packets to prioritize or how that choice gets made. In CDT’s view, outside the context of security threats, it is important that such choices be controlled by end users rather than by network operators. The existence of Diffserv as an approved Internet technology standard, in other words, does not in any way imply that discrimination by network operators should not be subject to careful safeguards and limits.

A number of commenters suggest, however, that current law already provides ample safeguards, making it unnecessary to take such further steps as enacting legislation or adding a fifth principle to the Commission’s Policy Statement. Some argue, for example, that a broadband plan should simply reaffirm the apparent Commission policy, reflected in the 2008 Comcast Order,¹⁶ of oversight based on case-by-case assessment and post-hoc enforcement, with no bright-line rules.¹⁷ Others point to antitrust law as adequate protection against forms of discrimination that are anticompetitive.¹⁸

Assessing differential treatment of Internet traffic on a case-by-case basis may make more sense than establishing detailed bright-line rules that could prove insufficiently flexible. At the same time, to be a good policy approach, case-by-case analysis needs to be guided by some set of standards or principles. Otherwise, it results in purely ad hoc decisionmaking, effectively vesting total discretion in the hands of whichever officials happen to be in power at the moment. This is why CDT advocates legislation to codify and cabin the oversight authority the Commission asserted in the Comcast Order; even those who like the decision’s results should have some concern about the scope of authority and discretion that the Order seems to assert. A better approach would be for

¹⁵ AT&T Comments at 105.

¹⁶ *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”).

¹⁷ *See, e.g.*, Comments of Cisco Systems, Inc. (“Cisco Comments”) at 18-20; AT&T Comments at 98-102.

¹⁸ NCTA Comments at 40.

statutes or regulations to establish principles – for example, the principle CDT offers above that congestion management tactics should be evenly applied based on objective standards, rather than allowing network operators to pick favorites. The application and enforcement of such principles could then be assessed on a case-by-case basis.

Antitrust law, meanwhile, is an important safeguard against anticompetitive conduct. But broadband policy should not merely aim to protect against bad behavior and the abuse of market power. Rather, maximizing broadband requires the preservation of an affirmative good: the Internet’s unique ability to serve as a platform for upstart innovation and hypercompetition in online services and applications. It is far from clear that decisions that chip away at the platform’s utility in fostering such competition would rise to the level of antitrust violations. For example, would the conduct at issue in the Comcast Order have supported a successful antitrust claim?

Moreover, as a practical matter, small upstart innovators are highly unlikely to be in a position to bring antitrust cases against major network operators. For any individual innovator facing a problem as it tries to roll out a product, it would likely be faster and more cost effective to go ahead and negotiate deals with ISPs than to litigate antitrust suits against them. But that kind of negotiation-and-permission prerequisite is precisely the kind of hurdle to innovation that broadband policy should seek to avoid.

2. Arguments Concerning Network Management

Many commenters stress that network management is needed to address various problems and challenges. As CDT has advised the Commission before, however, it does not follow that any and all actions taken in the name of network management are entirely benign, or that broadband policy should not call for principles and scrutiny to help shape (without dictating the details through prescriptive rules) the forms that network management will take.¹⁹

Some commenters argue that network management is needed to ensure quality of service. The idea is that certain applications, like advanced teleconferencing, may not be able to run on the public Internet without network management to give preference to its packets.²⁰ CDT believes there are risks, however, in allowing network operators to selectively determine which applications will get the major advantage of packet prioritization. If the power to grant such treatment lies exclusively with the network operator, it becomes the gatekeeper for new applications – because a would-be provider of an upstart application needs to work out a deal with the network operator in order to offer fully functional service. Once again, a better answer is to give control to users. Quality-of-service issues could be addressed by allowing *users* to select when and where special treatment is required. A prioritization system of that kind is something any

¹⁹ See Reply Comments of the Center for Democracy & Technology, *Broadband Industry Practices*, WC Docket 07-52 (Feb. 26, 2008)

(http://www.cdt.org/speech/20080228_FCC_comments.pdf) at 2-3.

²⁰ Cisco Comments at 17, 19; see also AT&T comments at 104, 106.

application provider could take advantage of, by communicating to users that they should select the service for priority designation.

Another cited purpose for network management concerns emergencies; for example, AT&T suggests that during a pandemic, a doctor's Internet connection to the hospital might need to be given priority over a neighbor's Web-surfing session.²¹ Emergency scenarios, however, should not be used to justify a broader ISP right to discriminate. As a general matter, ISPs should not be in the business of determining which communications are more important than others – the doctor's over the neighbor's, for example – and discriminating accordingly. And even in emergencies, it is not clear why an ISP needs or should have unfettered discretion to make ad hoc judgments about priority; at a minimum, CDT would argue that any prioritization should be done pursuant to objective and transparent criteria.

Some commenters further suggest that network management is needed to enable network operators to “differentiate” their services from competitors.²² In CDT's view, ISPs can and do seek to differentiate their services based on factors like bandwidth capacity, pricing options, and customer support. Differentiation based on the provision of excellent user-controlled prioritization or content filtering (e.g., parental controls) options is welcome as well. But it is not clear why differentiation should require an ISP, as opposed to its customers, to select Internet traffic for differential treatment. If the idea is that an ISP may try to “differentiate” various applications or add-on services it offers (teleconferencing, VOIP, etc.) by giving them faster or more reliable carriage on the network than non-affiliated offerings, CDT believes that is exactly the kind of behavior that nondiscrimination safeguards are designed to prevent. To the extent that “differentiation” means an ISP using discriminatory traffic routing to provide services or applications that competitors are unable to duplicate, that is just another way of saying that the ISP seeks to increase revenue by sheltering some of its online offerings from the full pressure of the Internet's hypercompetitive environment. That is not a goal the national broadband plan should aim to accommodate.

3. Applying Policy Statement and Nondiscrimination to Wireless

Commenters associated with providers of wireless communications services tend to argue that wireless broadband should not be subject to the Commission's broadband Policy Statement or to any other policies concerning openness or nondiscrimination.²³

CDT agrees with Verizon's observation that the wireless marketplace shows an encouraging trend towards increased openness, based on developments such as Verizon Wireless' Open Development Initiative and statements by other carriers that customers

²¹ AT&T Comments at 67-69.

²² Cisco Comments at 20; *See also* Verizon Comments at 88-89.

²³ Comments of CTIA – The Wireless Association (“CTIA Comments”) at 29-30; Verizon Comments at 96-111; AT&T Comments at 115-125.

may use third-party devices and applications.²⁴ Nonetheless, the wireless environment lacks the tradition of openness that has characterized the wireline Internet. There may be legitimate historical reasons for the different traditions. But in a converging world where wireless connectivity is expected to make broadband Internet access increasingly ubiquitous, failing to address wireless would leave a gaping hole in any policy meant to promote openness or nondiscrimination on the Internet.

The arguments for entirely exempting wireless broadband generally overstate what a sensible application of the Policy Statement or other additional nondiscrimination principles to wireless would mean. For example, they cite the need for active network management to juggle the challenges stemming from the shared use of limited radio spectrum, as if network management somehow might be precluded.²⁵ But no sensible version of policy in this area would bar wireless carriers from managing their networks to cope with capacity issues. Rather, it would simply require network management practices to comply with some core principles, such as being evenhanded rather than singling out specific applications for special treatment. That is very different from the outright “banning of packet priority.”²⁶

To take a concrete example, AT&T, citing capacity constraints, has not allowed the use on its 3G wireless network of applications that stream live television video, such as SlingPlayer. Yet in June, AT&T began to allow use of an application to stream live broadcasts of baseball games.²⁷ If extremely high bandwidth usage by users of streaming video applications poses a problem for a wireless network, it should be possible to devise network management parameters that employ objective and transparent standards for what will be allowed and what will be limited. There would be nothing wrong, for example, with limiting how much bandwidth individual users may consume during periods of congestion. But applying limits selectively – such as allowing some streaming video applications but not others, based on arbitrary or secret criteria – gives the network operator gatekeeper control.

Nor would applying openness requirements to wireless broadband mean “requiring every device to support every application” and banning specialized devices like the Amazon Kindle.²⁸ In the wireline world, there are devices built just for email. There is software written for one operating system but not others. There are cable television services delivering a single application (cable TV). None of this violates the Policy Statement, nor would it violate a new nondiscrimination requirement. The point of an openness requirement, for wireline as well as for wireless, would be to say that Internet service must be capable of being used with whatever devices and applications the user chooses – and without the carrier trying to steer the consumer’s choice via discriminatory

²⁴ Verizon Comments at 98-100; *see also* AT&T Comments at 119.

²⁵ *See* Verizon Comments at 105-106; AT&T Comments at 120.

²⁶ CTIA Comments at 33.

²⁷ *See* Marguerite Reardon, *Is AT&T playing gatekeeper to the Wireless Web?*, CNET News (Jun. 18, 2009) (http://news.cnet.com/8301-1035_3-10268319-94.html).

²⁸ AT&T Comments at 121-122.

transmission quality. This does not mean that *every individual device or service* must be open to all applications; consumers can freely choose single-purpose devices or non-Internet services like cable TV. It just means that more open, general-purpose devices and true Internet service should remain available as well.

Similarly, wireless openness, properly conceived, would not deny consumers the option of selecting a more “highly-managed network environment for their wireless devices.”²⁹ Just as a company in the wireline world can set up a Web site to host a pre-selected set of “trusted apps” for download, so ISPs or hardware providers like Apple could offer pre-screened applications for wireless customers. Applying openness requirements would merely ensure that wireless broadband Internet customers are not prevented from choosing to participate in a more open ecosystem, and that network operators do not discourage that choice by giving traffic associated with non-approved applications or devices lower priority in transmission.

Finally, regardless of whatever openness principles or requirements a broadband plan might extend to wireless broadband services generally, it should be clear that any government efforts to affirmatively support additional wireless broadband deployment should demand a substantial level of openness. Single-purpose or gatekeeper-managed networks should not be subsidized or otherwise specially supported as part of the plan. As stated in CDT’s initial comments, broadband is worth encouraging because of its ability to serve as basic infrastructure with unlimited uses and potential. More limited services may have a place in the marketplace, but they do not warrant the same kind of government support or resources.³⁰

4. Impact of Nondiscrimination on ISPs Fighting Copyright Infringement

Commenters with a strong interest in copyright argue that any nondiscrimination-oriented provisions included in a broadband plan must leave ISPs free to take active steps to deter or reduce copyright infringement on the network.³¹

CDT believes that the plan’s nondiscrimination policies or obligations should, consistent with current Commission policy as set forth in the broadband Policy Statement, apply

²⁹ Verizon Comments at 100-101; *see also* AT&T Comments at 122-124 (noting that “[u]sers may prefer the iPhone model, in which Apple has reviewed and approved the applications available in the iTunes App Store as being secure”).

³⁰ *See* CDT Comments at 5, 10-11.

³¹ *See* Arts+Labs Comments; Comments of the Walt Disney Company; Filing of the Songwriters Guild of America; Comments of the Entertainment Software Association; Joint Comments of American Federation of Television and Radio Artists AFL-CIO, American Society of Media Photographers, The Copyright Alliance, The Directors Guild of America, Graphic Artists Guild, The International Alliance of Theatrical Stage Employees, Motion Picture Association of America, Professional Photographers of America and Alliance of Visual Artists, Property Rights Alliance, Recording Industry Association of America, Screen Actors Guild.

expressly to *lawful* communications. For obvious reasons, unlawful communications do not merit such protection. The Commission should be wary, however, about affirmatively endorsing or encouraging action by network operators to actively scour networks for unlawful material.

Inevitably, ISP actions targeting unlawful communications will end up having some impact on lawful communications as well. For one thing, identifying unlawful communications is likely to require the inspection of a great quantity of communications that turn out to be perfectly lawful. Scrutinizing user communications on a widespread basis raises serious privacy issues. Consumers simply do not expect their ISP to be regularly examining the content of their Internet communications, and some will not use broadband to the full extent if they believe the ISP is doing so, just as they would be wary of the telephone if they believed all phone conversations were being wiretapped.

In addition, evaluating the legality of individual communications may be easier said than done. ISP efforts to identify unlawful communications might be countered by wider use of encryption – leading to an arms race between the ISP and its customers and ultimately slowing network performance due to increased computer processing demands. Just as important, technological tools, even as they grow more advanced, have little capacity to make judgments about tricky legal questions such as how to distinguish a “fair use” of copyrighted material from an infringing use. Where such judgment calls are required, ISP decisions could easily affect activities that a court might determine to be legal.

In short, to ask network operators to serve as policemen, judge and jury with respect to the legality of individual Internet communications is to advocate a fundamental recasting of the role of ISPs. It is far from clear that adopting this radically different model would have any positive effect on broadband. Rather, by putting ISPs in a more active gatekeeper role, it would risk significantly undermining the foundational and proven principles identified in CDT’s initial comments. The broadband plan should not go down this dangerous path.

5. The Role of Self-Regulation in Protecting Privacy

A number of commenters, while acknowledging that privacy is important for fostering the consumer trust that is essential for full utilization of broadband, argue that privacy issues are best addressed by self-regulation.³²

CDT believes strongly that self-regulation can play a significant role in building norms and expectations for the protection of privacy. The experience with self-regulation in this area however, is no better than mixed and meaningful progress tends to occur mainly when the threat of specific legislation or government regulation is imminent.

³² See, e.g., Chamber Comments at 8; Comments of the United States Telecom Association at 28-29.

For example, the Network Advertising Initiative (“NAI”), a self-regulatory group of online advertising networks, was formed a decade ago in response to pressure from the FTC and consumer advocates in the wake of privacy concerns over the merger of ad network DoubleClick and offline data broker Abacus. NAI represented an important first step at the time it was launched, but its approach also had some flaws that CDT and others identified as needing further work, such as a confusing and ineffective opt-out process. For years, the NAI neither made significant progress with regard to these flaws nor updated its principles to keep pace with evolving technology and industry practices. Late last year, amidst intensifying attention by the FTC and Congress to behavioral advertising and related privacy issues, NAI to its credit made some major improvements and updates to its framework. That same regulatory pressure more recently spurred the leading advertising-related trade associations to adopt their own self-regulatory principles.³³ Even with the welcome improvements, however, a number of outstanding substantive questions remain, and issues like implementation, compliance, transparency, and ongoing updates remain open questions.³⁴

Moreover, even an extremely strong self-regulatory regime cannot regulate the behavior of entities that choose not to participate. Companies that intend to engage in questionable or “grey area” practices are free to stay outside the regime, and their bad practices could undermine the trust in the medium that more responsible companies are working to try to build. For example, the NAI was for many years missing a number of important industry players.³⁵

For these reasons, CDT believes that a national broadband plan should call not just for self-regulatory efforts to protect privacy, but also for enactment of a baseline federal privacy statute and active Federal Trade Commission oversight, as discussed in our initial comments.³⁶ In addition, to address privacy concerns associated with government access to consumer data, the plan should call for reform of the outdated Electronic Consumer

³³ <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>.

³⁴ See CDT, *Response to the 2008 NAI Principles: The Network Advertising Initiative’s Self-Regulatory Code of Conduct for Online Behavioral Advertising* (Dec. 2008) (http://www.cdt.org/privacy/20081216_NAIresponse.pdf). The original NAI principles provided for independent audits and enforcement against non-compliant members, but the audit results were never made public and reporting on compliance with the principles was inconsistent. See Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007) (http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf) at 16-17.

³⁵ CDT testing in 2006 revealed that only a tiny fraction of companies that collect data that could be used for behavioral advertising were NAI members. See *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy? Hearing Before the Antitrust, Competition Policy and Consumer Rights Subcomm. of the Senate Comm. on the Judiciary* (Sept. 2007) (Statement of the Center for Democracy & Technology) (<http://www.cdt.org/privacy/20070927committee-statement.pdf>).

³⁶ CDT Comments at 12-16.

Privacy Act.³⁷ Self-regulation cannot provide a full solution to the privacy questions the Commission raised in its NOI in this proceeding.

* * *

CDT urges the Commission, as it develops a national broadband plan, to include provisions that endorse, affirm, and strengthen the characteristics that make the Internet uniquely open to free expression and independent innovation. Measures to spur broadband deployment and adoption are crucially important, but cannot yield their full potential benefits unless the Internet to which they provide access retains its open and innovative character.

Respectfully submitted,

Leslie Harris
David Sohn
John Morris
Alissa Cooper

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

July 21, 2009

³⁷ CDT Comments at 16-17.