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

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

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Leslie Harris
David Sohn
John Morris
Alissa Cooper
Andrew McDiarmid
Jonathan Dunn

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

January 14, 2010

Table of Contents

Summary

CDT commends the Commission's efforts in this proceeding to ensure that the Internet's open character is protected into the future. The Internet's extraordinary success stems directly from its openness to independent innovators and speakers. But in the absence of an appropriate policy framework, broadband Internet access providers could act in ways that substantially undermine the medium's openness.

The framework set forth in the NPRM is a good start, but CDT believes a number of modifications and clarifications are essential.

With respect to its assertion of **legal authority**, the Commission needs to go back to square one. The Commission's overall policy goal must be, to quote the NPRM, "to promote an Internet that is both open and unregulated." It is crucial, therefore, that the Commission's assertion of jurisdiction in this proceeding not pave the way for broad government regulation of Internet matters in the future. Unfortunately, the jurisdictional theories set forth in the NPRM are sweepingly broad and set no express limits on what the Commission can regulate on the Internet. The NPRM's unbounded assertion of legal authority raises statutory and constitutional concerns, would not survive judicial review, and is in direct conflict with the policy goals of this proceeding. It is particularly inappropriate for the Commission to base its authority here on 47 U.S.C. § 230.

CDT recommends that the Commission base its actions here on its authority under Title I to regulate transmissions by wire or radio. In setting forth this jurisdictional basis, the Commission should expressly state that it understands this authority to extend only to the provision of transmission functions – broadband Internet *access* service – and not to Internet matters generally. As an alternative basis for authority, the Commission could consider reclassifying broadband Internet access services as Title II services.

CDT strongly agrees that, in addition to codifying the existing four Internet principles, the Commission should add a **nondiscrimination principle**. But the proposed principle and its accompanying explanation should be modified in several ways:

- To avoid possible impact on benign activities like caching, the discrimination rule must be modified to focus expressly and exclusively on discrimination in the interior of a broadband provider's network – that is, at the level of the routers that control transmission.
- The Commission should make clear that the rule is not limited to discrimination motivated by direct payment or to discrimination that takes the form of enhancing certain transmissions; unpaid discrimination and degradation should be covered as well.
- The Commission should expand its explanation to clarify that actions based on a subscriber's service plan or bandwidth usage patters will *not* be treated as discrimination – so long as the actions do not hinge on the content, application, or destination of the subscriber's communications.
- The Commission should add a clear statement that the nondiscrimination rule will not prevent broadband providers from enabling *individual subscribers* to designate how their different traffic streams should be prioritized. Portable, user-directed prioritization carries none of the risks of discrimination at the discretion of broadband providers, and the Commission should encourage it.

CDT also strongly supports the addition of a **transparency** principle, with the following suggestions:

- Unlike the other rules, the transparency rule should not be subject to the "reasonable network management" exception. Disclosure of network management practices, including reasonable ones, is precisely what a transparency rule is for.
- The Commission should clearly state that transparency means making available sufficient information not just for subscribers, but also for developers of online applications and services, who need to understand how the broadband networks will work.
- The Commission should clearly differentiate between network management aimed at congestion and network management aimed at security. Transparency regarding congestion management tactics should include significantly more detail, since disclosure would not pose circumvention concerns.
- In addition to disclosures about network management, the Commission should require broadband providers to disclose how the bandwidth capacity they dedicate to Internet access service compares to the capacity they dedicate to managed or specialized services.

With respect to **reasonable network management**, CDT believes the Commission, in its final order, should include explanatory language providing some high-level guidance concerning what practices are likely to be deemed "reasonable." Technical bodies such as the IETF have an important role in setting standards that may be used for network management, but are not in a position to evaluate when particular management practices are "reasonable." Guidance must come from the Commission. An appropriate set of high-level principles would say that reasonable network management practices should be:

- Based on general criteria that are applied fairly and evenly, so that the network provider is not selecting which specific content or applications to favor or disfavor. For congestion management in particular, providers should use objective criteria such as volume of bandwidth usage. (A key test for reasonableness would be: does this tactic have equal impact on all applications with comparable bandwidth characteristics?)
- Consistent with the common technical standards on which the Internet's broad interoperability depends.
- Sufficiently transparent to both subscribers and developers of Internet applications and services.

In addition, the Commission should revise the rule's definition of "reasonable network management."

- The rule's references to preventing unlawful conduct should be deleted. Their inclusion is unnecessary, because the rules apply only to "lawful" transmissions in the first place. Meanwhile, encouraging broadband Internet access providers to take on new network policing functions would entangle the Commission in difficult legal and policy issues. It also would run contrary to the goals of this proceeding, which focus on preserving the Internet's successful model – a model in which network operators do not exercise centralized supervision or control.
- The rule's "catch-all" reference to "other" practices should be cabined.

With respect to **managed or specialized services**, CDT agrees that services that are *not* broadband Internet access should not be subject to the openness rules. But the NPRM's use of

the term “managed or specialized services” without providing any definition of the term carries major risk that the term could be misinterpreted in ways that create gaping loopholes in the open Internet rules. To prevent this, the Commission should:

- Add to the rules a definition of “managed or specialized services.” The definition should ensure that “managed or specialized services” will not be merely Internet services by another name (minus the openness).
- The definition must also ensure that “managed or specialized services” is not just a label that can be applied to whatever portion of Internet traffic a broadband provider may wish to prioritize. To achieve this, the definition must specify that “managed or specialized services” be carried on bandwidth that is distinct from bandwidth devoted to Internet traffic.
- The Commission should require periodic reporting of how providers’ bandwidth allocations for Internet access compare to their allocations for managed or specialized services. The Commission should make clear that if a provider’s Internet access is being neglected in favor of managed or specialized services, the agency will not hesitate to act, including reclassifing the provider’s services to bring them within the scope of the openness rules.

Finally, CDT agrees that the Internet openness rules should apply to all broadband Internet access service delivery platforms, including **wireless.** Wireless networks may require more aggressive traffic management to ensure the smooth and effective operation of the network. Nonetheless, reasonable traffic management in the wireless context should still focus on the amount of bandwidth being used, rather than singling out specific content, applications, services for special treatment. As an exception to this principle, the Commission may want to indicate that, for legacy reasons, prioritization of voice services will be considered reasonable for mobile wireless networks.

This proceeding presents an opportunity to ensure that the dynamic growth and innovation seen on the Internet over the past 15 years can continue. CDT looks forward to working with the Commission to refine its proposed rules.

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

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

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 Proposed Rulemaking (NPRM), FCC 09-93, regarding proposed rules to preserve the free and open Internet.[1] CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet – a mission that closely tracks the Commission's goals for this proceeding.

I. Introduction

The Internet's extraordinary success in facilitating independent innovation and speech is directly linked to the fact that any Internet user can provide content and services to any other willing Internet user, without getting permission from any "gatekeeper." An individual or small start-up company can buy a connection from a single provider of broadband Internet access and immediately reach the whole of the Internet. This keeps barriers to entry low and makes the Internet uniquely open to innovation, competition, and speech.

CDT strongly commends the Commission for recognizing the central importance of Internet openness to modern communications policy and for working in this rulemaking to ensure that the medium's open character is protected into the future.

This proceeding rightly focuses on creating a basic regulatory framework to protect against the risk that network operators could engage in behavior that would undermine this characteristic openness. The overall policy goal in this area, however, must be, as the NPRM suggests in paragraph 47, "to promote an Internet that is both open and unregulated." It is crucial, therefore, that the Commission's actions and statements in this proceeding not pave the way for broad government regulation of Internet matters in the future. The Commission must base its decision here on a careful and expressly limited assertion of its regulatory jurisdiction. The NPRM's proposed assertion authority is not suitably limited and should be carefully revised as described below.

[1] Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191 (proposed Oct. 22, 2009) (to be codified at 47 C.F.R. pt. 8) [hereinafter "NPRM"].

The Commission rightly proposes that rules to protect Internet openness should be high-level, rather than prescribing behavior in significant detail.[2] In a number of areas, however, CDT believes the Commission should provide more guidance than is contained in the NPRM. In some cases, CDT recommends specific amendments to the proposed rules; in others, CDT suggests that the Commission offer clear explanatory language in a final order. These comments offer CDT's views, on an issue-by-issue basis that tracks the organization of the NPRM, on how to convert the NPRM's promising start into a workable and effective policy regime for protecting the Internet's open character.

II. The Need for Commission Action

A. Action is warranted

CDT agrees with the Commission's assessment that action is warranted to safeguard the Internet's open character. CDT has long argued, in various papers and in a number of comments to the Commission, that the future of the Internet model – the model enabling speech and innovation without permission – is not guaranteed.[3]

There are a host of concerns and problems that support action to ensure openness, and we will only briefly mention some of them here. History shows that private-sector owners of communications networks often resist innovations that reduce their control over how their networks are used. AT&T famously opposed allowing customers to use non-AT&T telephone equipment until forced to do so by the Commission's *Carterphone* decision.[4] More recently, when cable modem providers came along in the 1990s, they originally blocked streaming video applications.[5] Meanwhile, the marketplace for broadband Internet access in most U.S. localities today offers limited choices, a far cry from the crowded pre-broadband marketplace featuring thousands of providers offering dial-up Internet access over the common carriers' telephone

---

[2] *See* NPRM ¶¶ 12, 49, 89.

[3] *See Reply Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future*, GN Docket No. 09-51, July 21, 2009, http://www.cdt.org/files/pdfs/20090721_fcc_broadband_comments_3.pdf; *Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future*, GN Docket No. 09-51, June 8, 2009, http://www.cdt.org/files/pdfs/20090608_broadband_comments.pdf; *Reply Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, Feb. 28, 2008, http://www.cdt.org/files/pdfs/20080228_FCC_comments_2.pdf; *Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, Feb. 13, 2008, http://www.cdt.org/files/pdfs/20080213_FCC_comments_1.pdf; *Reply Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, July 16, 2007, http://www.cdt.org/files/pdfs/20070716fcc-comments.pdf; *Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, June 15, 2007, http://www.cdt.org/files/pdfs/20060615fcc-neutrality.pdf; *Comments of the Center for Democracy & Technology In regards to the FTC Broadband Connectivity Competition Policy Workshop*, Project No. V070000, Feb. 28, 2007, http://www.cdt.org/files/pdfs/200702028ftcneutrality_1.pdf; Center for Democracy & Technology, *Preserving the Essential Internet* (June 2006), http://www.cdt.org/files/pdfs/20060620neutrality_1.pdf; Jerry Berman & John B. Morris, Jr., Center for Democracy & Technology, *The Broadband Internet: The End of the Equal Voice?*, Computers, Freedom & Privacy Conference (Apr. 2000), *available at* http://www.cdt.org/files/pdfs/broadbandinternet_2.pdf.

[4] *Use of the Carterphone Device in Message Toll Telephone Service*, 13 FCC 2d 420 (1968).

[5] JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 173 (2005). Marketplace pressures forced cable modem providers to change this policy, but they faced competition from DSL providers subject to common carriage rules and numerous narrowband ISPs, which at that time were still a significant factor in the market. Today, many consumers have only two viable choices for broadband, and neither is required to offer a nondiscriminatory platform.

lines. Furthermore, many of the current broadband providers have or are seeking to add substantial interests in content or services that may face competition from independent online offerings. Providers of broadband Internet access may therefore have the ability and incentive to engage in practices that create a measure of gatekeeper control and leave the Internet less open. Beyond such practices, certain kinds of responses to legitimate network issues such as congestion can have a similar impact, even unintentionally.

Perhaps most crucially, if providers of broadband Internet access were to adopt practices that undermine the openness of the Internet, it would likely be extremely difficult to reverse the damage after-the-fact. Unraveling a web of discriminatory deals after significant investments have been made and business plans built would be a difficult and complicated undertaking both logistically and politically. It could also be difficult to document the harms to innovation – nobody knows about small businesses and innovative applications that are lost before they make if off the ground.

B. Responses to certain arguments against Commission action

1. Needs of access providers to recover costs

The NPRM cites the argument that charging content, applications, and service providers may be necessary to recover the costs of deploying and upgrading broadband networks, or to defray the amount of those costs falling on end users.[6] But the costs associated with a broadband network need not be borne by Internet access services alone. It is common today for network operators to offer "bundles" of services over a single physical network, including but not limited to broadband Internet access. As discussed below, CDT believes broadband providers should be permitted to offer non-Internet services as "managed or specialized services" that, while segregated from Internet traffic from a bandwidth capacity perspective, use the same physical infrastructure and hence help cover its costs. For example, network operators have long offered private transmission or "virtual private network" services to enterprise customers, and nothing in the Commission's proposed rules would prevent them from continuing to seek additional revenues from such services.

Moreover, to the extent that costs are driven up by a small group of subscribers using extraordinary amounts of bandwidth, it would be perfectly reasonable for broadband providers to raise charges for such users. The NPRM cites opponents of regulation in this area as noting that price signals ideally should reflect the congestion costs of bandwidth-sensitive applications[7] – but the root cause of misaligned price signals is subscriber service plans that purport to offer entirely unlimited bandwidth and hence create no incentive for users or applications to economize on bandwidth usage. The Commission's proposed Internet rules would in no way interfere with the ability of broadband Internet access providers to create better incentives by making "bandwidth hogs" pay proportionate costs.

Providers of broadband Internet access do not appear to be in dire financial straits. They offer a service that clearly is of increasing utility to consumers, as more and more commercial, social, and civic activity moves online. There is no reason to believe, therefore, that providing broadband Internet access service to paying subscribers is not a viable business. Access

[6] NPRM ¶ 65.
[7] *Id.*

providers may need to modify the current "all-you-can-eat" pricing model, but that is a matter entirely within their control and beyond the scope of any proposed regulation.

2. Two-sided markets

The NPRM notes that some opponents of Commission action in this area point to economic arguments regarding "two-sided markets."[8] Embracing the concept of a two-sided market in the Internet access service context would be inconsistent with preserving the Internet's openness, and would be contrary to the historical structure of financial relationships on the Internet – a structure that has directly contributed to the extraordinary innovation we have seen over the Internet's short life.

The Internet is a user-driven medium. For providers of broadband Internet access, the end user subscriber is the customer, and end users control how and for what purposes they will use the service. This user-centric focus would change if broadband Internet access providers start thinking of themselves as providing transmission services not just to end user subscribers, but also to non-subscribers such as large online content providers to whom they do not directly provide bandwidth. Creating a two-sided market means dividing the broadband providers' loyalties and creating a new set of incentives beyond just empowering subscribers.

Selling priority treatment to online content providers could mean that, in exchange for a fee, the broadband provider effectively would be steering its subscribers towards particular content, applications, or services (by making them faster or more reliable) and away from others. This would be very different from the way a two-sided market works in the newspaper context, to take a commonly cited example. The inclusion of paid advertisements in newspapers presumably has minimal impact on how non-advertisement portions of the newspaper are perceived by or presented to readers. Paid priority on the Internet would be akin to a newspaper market in which advertisers pay fees not just to run ads, but to influence the placement of substantive articles – determining which articles appear on the front page and which on the interior pages, for example.

In the Internet context, this kind of two-sided market would create major problems for independent innovators. Broadband Internet access providers have a termination monopoly with respect to their subscribers. An innovator seeking to offer some new content, application, or service to a consumer has no choice but to reach that consumer through the consumer's broadband Internet access provider. The Internet is open today because that Internet access provider, by carrying any traffic the subscriber requests on essentially nondiscriminatory terms, is not exercising bottleneck control. By contrast, in a two-sided market, the treatment the innovator's traffic gets would depend at least in part on whether it had struck a deal with the broadband access provider.

Indeed, the central concept of a two-sided market involves *negotiating to reach an audience.* The Internet is an open platform precisely because it requires no such negotiation. Turning the Internet into a two-sided market would make it dramatically less open, less innovative, and ultimately less empowering of users.

[8] *Id.* ¶ 66.

3. Antitrust law

The NPRM also asks whether generally applicable antitrust laws may sufficiently address the concerns raised in this proceeding.[9] CDT believes that relying solely on antitrust law would be a serious mistake.

Antitrust law provides an important safeguard against anticompetitive conduct. But the goal in this proceeding is not merely to protect against anti-competitive behavior and the abuse of market power. Rather, the aim is to preserve an affirmative good: the uniquely open network structure that has enabled the Internet to serve as a platform for upstart innovation and independent speech. The benefits of that structure include non-economic considerations such as social and civic empowerment.

It is very doubtful that existing antirust law would cover the full range of potential threats to the preservation of this open structure.[10] Certain practices by broadband providers might lack any obvious anticompetitive purpose; they might have justifications tied to competitively-neutral purposes such as controlling congestion (as Comcast claimed in the Comcast-BitTorrent dispute[11]). Some practices might have no discernable impact on existing competitors in any specifically identified market – but might nonetheless leave the platform generally less open to future innovation, including in markets that may today not even exist.

In addition, individual practices with no clear anticompetitive motivation or impact could have the cumulative effect of undermining openness. Suppose a provider of broadband Internet access were to strike deals with many content providers for priority treatment. It is far from clear that the individual deals would be unlawful under current antitrust law. But if such deals become sufficiently commonplace, unprioritized traffic might find its performance degraded, because it would always be "last in line" behind all the prioritized traffic. The cumulative effect would be to make deals with broadband providers a practical necessity for many purposes – precisely the kind of result that this rulemaking aims to avoid.

For antitrust law to impose an affirmative obligation on broadband providers to maintain and operate their networks only in ways that preserve the paradigm of openness, it would probably be necessary to invoke some version of the "essential facilities" doctrine. But such an approach might well not succeed under current law. The Supreme Court has never recognized the doctrine and Federal courts are hesitant to embrace it.[12]

---

[9] *Id.* ¶ 81.

[10] *See* Susan Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 919 (2009), *available at* http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume89n3/documents/CRAWFORD.pdf ("Antitrust law, with its single-minded focus on firms competing in established markets, is ill-equipped to deal with discrimination by providers of physical transport networks for Internet access."). *See also* James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15, 17-21 (2003), *available at* www.luc.edu/law/activities/opportunities/docs/ljc2003/**speta** revised.pdf (detailing the problems of relying solely on antitrust law in this space).

[11] *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, 23 FCC Rcd 13028, ¶ 47 [hereinafter "Comcast Opinion and Order"].

[12] *See Verizon Commc'ns, Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 410-11 (2004) ("We have never recognized [an "essential facilities"] doctrine, and we find no need either to recognize it or to repudiate it here."); Speta, *supra* note 10, at 20 ("antitrust courts are less vigorous in their embrace of claims (such as 'essential facilities' claims) that would force a company with natural market power to open its property or business to others").

Finally, as a practical matter, individual innovators and small startup companies are 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 probably be faster and more cost effective to go ahead and negotiate deals with broadband providers than to litigate antitrust suits against them. But that kind of negotiation-and-permission prerequisite is again precisely the kind of hurdle to innovation that this proceeding seeks to avoid.

Moreover, the prospect of that choice (between litigation and negotiation) would by itself be sufficient to stop some innovation. Some innovations on the Internet have blossomed even though their inventors did not have a commercial goal – and such innovators might well simply forgo the innovation rather than have to bother with *either* litigation or negotiation.

C. Issues regarding scope and terminology

CDT agrees strongly with the NPRM's statement that the rules at issue in this proceeding "address users' ability to *access* the Internet and are not intended to regulate the Internet itself."[13] Indeed, as discussed below, extending regulation to a broader set of Internet activities would likely exceed the Commission's legal authority. Entities that do not provide last-mile broadband Internet access services to end users are simply outside the proper scope of this proceeding.

CDT generally agrees with the NPRM's definition of "broadband Internet access," although we propose a minor modification to the definition to ensure a clear distinction between broadband Internet access and separate, non-Internet transmission services which fall within our proposed definition of "managed or specialized services."[14]

The NPRM asks to what extent the issues raised by this proceeding are dependent on the state of competition in markets for broadband Internet access service.[15] CDT believes that the reasons for action here do not hinge on detailed competition analysis. Nothing about this rulemaking should be conditioned on extensive fact-finding regarding the state of competition.

It should be clear that, for the foreseeable future, consumers in most local markets in the United States will face limited choices for broadband Internet access. A full analysis might well show some competition; two or even three rivals may compete vigorously in some markets on factors such as price and speed. But the marketplace will not look anything like the old market for dial-up Internet access, when there were literally thousands of providers and common carriage rules on the underlying phone network enabled new entrants to enter the market easily.

In the broadband market, it remains entirely possible that a small number of providers, even if competing on price or capacity in particular markets, could each make the judgment that it is not in its interest to maintain the Internet's traditional level of openness. They might, in other words, decide they want more control. Competition among a few providers may offer some protection against sudden, radical changes to the way the Internet operates, but it provides no guarantee against more gradual erosion of the Internet's open character.

[13] NPRM ¶ 14 (emphasis in original).
[14] *See infra* Part VIII.
[15] NPRM ¶ 81.

Moreover, even where a consumer enjoys two or more choices of broadband Internet access providers, the provider she ultimately chooses still has a termination monopoly. Any content, application, or online service seeking to reach that consumer must transit the facilities of the chosen access provider. More extreme forms of abuse of that monopoly (e.g., blocking a highly popular Web site or service) might prompt some consumer backlash, but a consumer is not likely to go through the substantial hassle of switching broadband Internet access providers simply because particular content seems a bit slow or because some new start-up service is not readily available. In short, competitive choices for *consumers* of broadband Internet access cannot ensure a fully open, competitive environment for *online innovators*.

Finally, two matters of terminology warrant discussion. First, the NPRM's definition of the "Internet" is close to being accurate, but unfortunately is not. In footnote 103, the NPRM states:

> [W]e propose to define the Internet as the system of interconnected networks that use the Internet Protocol for communication with resources or endpoints (including computers, webservers, hosts, or other devices) that are reachable, directly or through a proxy, via a globally unique Internet address assigned by the Internet Assigned Numbers Authority. . . . To be considered part of the "Internet" for this proceeding, *an Internet end point must be identified by a unique address assigned through the Internet Assigned Numbers Authority or its delegate registry*, not an address created by a user for its internal purposes.[16]

The problem is that some broadband service providers are using "carrier-grade NAT" (or "natural address translation") to assign *private*, non-globally unique IP addresses to their residential customers.[17] Thus, for example, DSL customers in some parts of Maine are assigned IP addresses in the *private*, non-IANA-assigned 192.168.x.x. range, and thus those customers (and their broadband service providers) would not be covered by the FCC's rules.[18] We have suggested revised language in the footnote to address this concern while (we hope) remaining consistent with the Commission's intent.[19]

Second, the NPRM frequently uses the term "quality-of-service" (and sometimes "quality of service" without the dashes) in a manner that risks creating significant confusion – and in that

---

[16] NPRM ¶ 48 n.103 (emphasis added).

[17] For a discussion of Carrier-Grade NAT, see Jeff Doyle, *Understanding Carrier Grade NAT*, NETWORK WORLD, Sept. 4, 2009, http://www.networkworld.com/community/node/44989.

[18] One of the undersigned authors of these comments has personal knowledge of the DSL IP address assignments in Maine.

[19] The Commission could use the following definition:

> For purposes of this proceeding, we define the Internet as the system of interconnected networks that use the Internet Protocol for communication with resources or endpoints (including computers, webservers, hosts, or other devices) that are reachable, directly or through a proxy or gateway, via a globally unique Internet address assigned by the Internet Assigned Numbers Authority (IANA). To be considered part of the "Internet" for this proceeding, an Internet end point must either be identified by a unique address assigned through the IANA or its delegate registry, or be reachable through a private address assigned by a broadband service provider. This definition shall not include addresses created by a user or on a user's premises for the user's internal network purposes. We do not intend for this definition of the Internet to encompass private intranets generally inaccessible to users of the Internet, or private networks that are typically created within residences behind carrier-provided gateways.

confusion, potential for loopholes to the Commission's rules. The term "quality-of-service" (often "QoS") is both a specific engineering term and a specific telecom-business term, with at times differing meanings in the two contexts. It seems possible that the NPRM's use of the term is not precisely referring to the meaning from *either* context. In engineering terms, QoS often refers to particular protocols or techniques intended to deliver a guaranteed level of service, a superior level of service, or sometimes both a guaranteed *and* superior level of service.[20] In business terms, QoS often refers to specific targets or conditions in contractual "service level agreements" (SLAs), almost always in commercial (*i.e.*, non-residential) telecommunications service contracts.[21] Yet the NPRM appears to use the term often to refer to a more general concept of "service quality" (essentially meaning the extent to which a customer's Internet access may be slowed or otherwise impaired by factors such as congestion)[22] We urge the Commission to avoid the term "quality of service" (with or without the dashes), because it has a number of precise but differing meanings, in favor of more generic language to describe what the Commission means.

III. The Commission's Authority To Prescribe Rules Implementing Federal Internet Policy

A. The Commission must assert a narrow and focused basis for jurisdiction

The Commission is commendably seeking to protect the Internet's openness from threats posed at the last-mile bottleneck. Equally commendably, the Commission has proclaimed a narrow and focused goal, stating that its proposed rules "address users' ability to *access* the Internet and are not intended to regulate the Internet itself."[23]

Unfortunately, the statutory provisions the NPRM cites as bases for legal authority are broad and general statements of policy regarding the Internet – suggesting that even if the current NPRM is narrowly aimed, the Commission is asserting sweeping authority over the Internet more broadly. Such broad authority, if upheld, would itself pose a serious threat to the Internet's openness and vitality. It is essential that the Commission step back and base its efforts to protect Internet openness on narrow and limited authority, to coincide with the asserted narrow focus of the NPRM on *access* to the Internet.

There are strong policy arguments for the Commission to assert only a very narrow authority in the Internet context. Moreover, as detailed below, the jurisdictional hooks used by the Commission – most importantly, Section 230 – do not support FCC action in this proceeding and would not survive appellate review. As an alternative to overly broad jurisdiction claims, we believe that the Commission can implement its proposed rules based on Title I of the Communications Act, so long as its assertion of jurisdiction is expressly limited to authority over the *transmission facilities* on which the broadband Internet rides, with the expressly limited aim

---

[20] For engineering discussions of QoS techniques, see, e.g., G. Huston, *Next Steps for the IP QoS Architecture*, IETF RFC 2990 (2000), http://tools.ietf.org/html/rfc2990; ITU-T, *Terms and Definitions Related to Quality of Service and Network Performance Including Dependability*, Recommendation E.800 (1994), *available at* http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2008-ttnfa2009/Belhachemi-Arab/files/IUT-T%20E800.pdf.

[21] *See, e,g.*, R. Garg et al., *A SLA Framework for QoS Provisioning and Dynamic Capacity Allocation*, Tenth IEEE International Workshop on Quality of Service (2002), *available at* http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1006581.

[22] *See, e.g.*, NPRM ¶ 108.

[23] *Id.* ¶ 14 (emphasis in original).

of protecting *access* to the Internet. With this approach, the Commission can implement the openness rules it proposes, while at the same time making clear to both reviewing courts and future Commissions that the Internet must remain "unfettered by Federal or State regulation."[24]

1. Policy and constitutional arguments for narrow jurisdiction

For this rulemaking to achieve its goal of safeguarding the open and unregulated Internet,[25] it is essential that the FCC articulate a narrow and limited jurisdictional basis for its action in this proceeding. A critical goal in this proceeding is to protect the dynamic innovation that the open Internet has fostered. But just as private gatekeepers can hinder innovation and the flow of Internet communications, so can overreaching government oversight and regulation. The Commission must be sensitive to both risks in crafting rules in this proceeding.

a. Broad jurisdiction would undermine the goals of this proceeding

In the absence of a clear legislative grant of authority, the FCC must not try to assert what would amount to unbridled discretion to regulate all aspects of the Internet. The FCC should focus narrowly on the risk of gatekeeper control by those who provide the physical network access connections. In other words, the limited basis for authority should focus solely on the provision of actual transmission capabilities, not the numerous services, applications, and content that may travel over those Internet connections. While the NPRM recognizes this – appropriately focusing specifically on the provision of broadband Internet access[26] – nothing in the Commission's broad jurisdictional theory would so limit the Commission's authority. Although this Commission may today be appropriately aware of the harm that regulation could have on the dynamic innovation that has been the hallmark of the Internet, future Commissions may not be so sensitive. If the FCC asserts broad jurisdiction over the Internet here, this rulemaking could have the effect of paving the way for broader future regulation of the Internet generally.

Thus, any assertion of jurisdiction that could be read to imply or support open-ended FCC regulatory authority would directly undermine the policy goals of this proceeding. Asserting clear *limits* to the FCC's reach is just as important to the long-term success of this proceeding as asserting authority. To truly safeguard an open Internet, the FCC's jurisdictional statement must aim to serve as a bulwark against broader Internet regulation in the future, not lay the groundwork for it.

In addition, as Commissioner McDowell's statement observes, foreign countries are looking to the United States action "to help justify an increased state role over Internet management internationally."[27] To avoid risking such a result, the FCC decision must be very clear in articulating a narrow and limited jurisdictional basis for any FCC action here.

b. Constitutional limits to the Commission's authority

As the Commission is aware, there are strong constitutional constraints on the regulation by the government – including the FCC – of Internet communications, particularly regulations based on

[24] 47 U.S.C. § 230(b)(2).
[25] *See* NPRM ¶ 47 ("[I]t has long been U.S. policy to promote an Internet that is both open and unregulated.").
[26] *See id.* ¶¶ 90-94.
[27] NPRM, Statement of Commissioner Robert M. McDowell Concurring in Part, Dissenting in Part.

the content of communications.[28] Regulations based on the content of communications are presumptively invalid.[29] In crafting any rules in this proceeding, the Commission must clearly avoid these constitutional limits, and it should ensure that its jurisdictional analysis does not invite unconstitutional actions by later Commissions.

The applicable constitutional constraints are at their strongest with the Internet. In *Reno v. ACLU*, the Supreme Court held that communications over the Internet warranted the full protection of the First Amendment.[30] Courts have repeatedly struck down as unconstitutional a range of governmental regulations of Internet content.[31] As courts have found, in the Internet context the *users* have great ability to control their Internet experience, and thus there is no strong reason for the government to step in to regulate Internet content or applications.[32]

The critical relevance in this proceeding of this analysis is the simple fact that almost all aspects of Internet communications are fully protected by the First Amendment, and thus there are strict constitutional limits on any regulation of Internet communications beyond the underlying transmission services. On the Internet, all of the data contained in communications between two Internet endpoints is protected speech, and hence cannot generally be regulated.

An analogy between a phone call and website visit can illustrate the protected nature of Internet communications. Although the FCC can regulate the underlying lines that allow a user to telephone a local movie theater to ask for show times, the FCC is precluded from regulating conversations that take place between the user and the theater. The user instructs her local device (a telephone) to interact with the underlying regulated network to connect a call to the theater, but what is exchanged over that connection is protected speech. Similarly, when an Internet user instructs her local device (a computer) to interact with her access provider and the Internet to connect with a movie theater's website (or a search engine, social network, or video site, etc.), the interaction between the user and the other end point on the Internet is constitutionally protected.[33]

---

[28] *See, e.g., Motion Picture Ass'n of Am. v. FCC*, 309 F.3d 796, 805 (2002).
[29] *See R.A.V. v. City of St. Paul*, 505 U.S. 377, 391 (1992).
[30] *Reno v. ACLU*, 521 U.S. 844, 870 (1997).
[31] *See, e.g.*, *Reno*, 521 U.S. 844; Ashcroft v. ACLU, 542 U.S. 656 (2004); *PSINet, Inc. v. Chapman*, 362 F.3d 227 (4th Cir. 2004); Am. Booksellers Found. v. Dean, 342 F.3d 86 (2d Cir. 2003); *Cyberspace Commc'ns, Inc. v. Engler*, No. 99-2064, slip op. (6th Cir. Nov. 15, 2000), *aff'g*, 55 F. Supp. 2d 737 (E.D. Mich. 1999); *ACLU v. Johnson*, 194 F.3d 1149 (10th Cir. 1999).
[32] The *Pacifica* case does not alter the conclusion that regulating Internet speech would be outside of the FCC's authority. FCC v. Pacifica Found., 438 U.S. 726 (1978). That decision turned on particular characteristics of the broadcast medium as it existed in the 1970s, and is wholly inapplicable to the Internet access context in the twenty-first century. The *Pacifica* Court itself "emphasize[d] the narrowness of [its] holding." *Id.* at 750. There are many key differences between broadband Internet access and the radio station at issue in *Pacifica*. First, unlike with broadband, the "users" in *Pacifica* (the radio listeners) were unable to shield themselves from unwanted radio content (apart from turning off the radio itself). At the time of *Pacifica*, radio devices did not have the capability to allow user control of access to content. In contrast, Internet access devices have substantial internal computing capability that allows them to operate user control software. Moreover, unlike in *Pacifica* (when a listener could be "assaulted" by content immediately upon turning on the radio), Internet access is inherently proactive, requiring a user to take affirmative steps to access content (and allowing ample opportunity for filtering software to be turned on prior to accessing content). These critical differences are at the core of the constitutional analysis, and lead to the conclusion that *Pacifica* would not support regulation of Internet communications – a conclusion the Supreme Court specifically reached in *Reno*. *See Reno*, 521 U.S. at 866-67.
[33] Paragraph 101 of the NPRM asks whether the Commission should seriously consider one commenter's suggestion that the Commission extend open Internet rules to search engines and other online services. Such an action would

From a constitutional perspective, it is vital that the Commission target its actions, and its assertion of jurisdiction, narrowly on interference with the *transmission* of communications, and avoid jurisdictional assertions that raise the specter of regulation of the communications themselves.

2. The NPRM's jurisdictional assertions are broad and unbounded, and would not survive review

The jurisdictional bases asserted by the Commission[34] are sweepingly broad and set no express limits on what the Commission can regulate on the Internet. In addition to being contrary to the policy goals of this proceeding and constitutional constraints on FCC action, such unbounded claim of authority is certain to lead to problems on possible appellate review. The NPRM's current claims of authority are unsupportable.

a. Section 230(b) provides no basis for Commission authority

The leading jurisdictional hook advanced in the NPRM is Section 230(b),[35] which sets out a series of broad Congressional policies about protecting and promoting the innovative openness of the Internet. But there is no assignment of authority to – or indeed even any mention of – the FCC anywhere in § 230. To imply FCC jurisdiction based on the broad policy statements in § 230 would be to suggest that the Commission could regulate virtually any aspect of the Internet. Not only would this result be clearly contrary to the meaning and intent of the statutory section, it would conflict with clear judicial guidance on the Commission's ancillary jurisdiction.

In passing 47 U.S.C. § 230 in 1996, Congress enacted a sweepingly *deregulatory* law. The entire purpose of § 230 was to remove legal and regulatory threats that were inhibiting development of the Internet generally, and of "user empowerment" technology in particular. For the FCC to rely on § 230 as a basis for *extending* its regulatory authority reach the Internet would simply turn the statutory provision on its head.

Section 230 advances three distinct legislative goals, and uses three separate operative provisions to achieve those goals.[36] Section 230(c)(1) sought to promote a vibrant and unfettered market for Internet content and services, and did so by *removing* a key barrier to innovation – the threat of liability for content posted by users and others. Section 230(c)(2)(A) sought to promote voluntary self-regulation of Internet content, and did so by *eliminating* a key disincentive to such efforts. Section 230(c)(2)(B) sought to promote the development of "user empowerment" tools, and did so by *removing* legal risks created by that development. Nothing in § 230 suggests that it also had as a purpose to increase regulation or the regulatory authority of the FCC over the Internet.

---

squarely raise serious constitutional concerns, and would, in any event, be far outside of the jurisdictional authority of this Commission.

[34] *See* NPRM ¶¶ 83-86.

[35] *See id.* ¶ 84 (citing 47 U.S.C. § 230(b)).

[36] For a full discussion of the three distinct goals and operative provisions of Section 230, see Brief for Anti-Spyware Coalition et al. as Amici Curiae Supporting Appellee, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009) (No. 07-35800), *available at* http://www.cdt.org/privacy/spyware/20080505amicus.pdf.

The deregulatory intent of Congress is made clear in the "findings" and "policy" provisions of § 230. One Congressional finding specifically noted the absence of regulation as a factor in the growth of the Internet:

> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, *with a minimum of government regulation*.[37]

Congress then went on to affirmatively state its intent *not* to regulate the Internet:

> It is the policy of the United States—
> . . .
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation* . . . .[38]

As the text of § 230 makes clear, Congress was not seeking to pave the way for more federal regulation of the Internet, or to hand the FCC a broad mandate over the Internet.

That non-regulatory intent is even more clear in the somewhat blunt statements of a lead sponsor of H.R. 1978,[39] the 1995 bill that was the legislative source of Section 230. Congressman Cox plainly stated that he did *not* want the FCC regulating the Internet. According to Cox, a critical goal of Section 230 was to:

> . . . establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government.
> . . .
> If we regulate the Internet at the FCC, that will freeze or at least slow down technology. It will threaten the future of the Internet. That is why it is so important that we not have a Federal computer commission do that.[40]

For the Commission to rely on Section 230 as a basis for any jurisdiction over the Internet is plainly antithetical to the intent of Congress in crafting that statute. And the U.S. Supreme Court has made clear in *FCC v. Midwest Video Corporation* that the Commission's ancillary jurisdiction cannot be used to justify or support regulatory actions that are in direct tension with the statutory scheme to which they are ancillary.[41] Simply put, the Commission cannot rely on § 230 to do something – assert jurisdiction over the Internet – that is directly contrary to the language and intent of § 230.

---

[37] 47 U.S.C. § 230(a)(4) (emphasis added).
[38] 47 U.S.C. § 230(b)(3) (emphasis added).
[39] Internet Freedom and Family Empowerment Act, H.R. 1978, 104th Cong. (1995), *available at* http://thomas.loc.gov/cgi-bin/query/z?c104:h.r.1978:.
[40] 141 CONG. REC. H8470–71 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox).
[41] *FCC v. Midwest Video Corp.,* 440 U.S. 689, 708-09 (1979).

On the other hand, as an important aside, although § 230 plainly does not provide a jurisdictional foundation for the FCC to assert authority over the Internet, is also does not *prevent* the Commission from regulating the transmission facilities that underlie the Internet. This conclusion should be clear from the context in which § 230 was enacted. At that time, in 1996, the Internet existed almost entirely riding on top of a highly regulated – and strictly neutral – network, the public switched telephone network. By enacting § 230, Congress made clear that *the Internet* could not be regulated, but at the same time Congress knew full well that the transmission platform on which the Internet was based *was* regulated, and Congress took as a given the Internet would still have a neutral transmission platform on which to flourish. Regulating the underlying transmission platform to maintain its neutrality would not be in tension with the intent or language of § 230, and indeed would – as the Commission has noted in other proceedings[42] – be consistent with the policy objectives expressed in § 230.

b. Reliance on Section 706(a) and Section 201(b) is also not appropriate

As with Section 230, Section 706(a) and Section 201(b) also do not provide a basis for ancillary jurisdiction over Internet access or communications.[43] Section 706(a) of the Telecommunications Act of 1996 charges the Commission with "encourag[ing] the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans,"[44] but the specific assignment to the FCC is limited to the use of certain specified tools such as "price cap regulation." In other words, even if § 706(a) is viewed as a grant of jurisdiction authority,[45] that grant is not broad enough to encompass the rules being promulgated in this proceeding. Moreover, any authority granted to the FCC by § 706(a) is most appropriately understood to mean that the FCC should encourage the deployment of transmission capabilities, not that the Commission has general Internet regulatory authority that would allow it to regulate how those capabilities are used.

Similarly, Section 201(b) is also not an appropriate basis for ancillary jurisdiction. At most it gives the FCC authority to carry out other *specific* provisions of the Communications Act (and the Commission has not named the provisions it is implementing under § 201).[46] Read more broadly than that, § 201(b) would be unbounded in its grant of authority to the FCC, and such a conclusion would – like § 230 – be contrary to the goals of this proceeding and would not survive appellate review.

---

[42] *See, e.g.*, *Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, 19 FCC Rcd 3307 (2004); *Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, 19 FCC Rcd 22404 (2004). These orders note the consistency between the policies articulated in § 230 and the particular Commission actions in those proceedings, but they do not squarely rely on § 230 as the basis for jurisdiction for the FCC actions (as the NPRM here does). In the *Vonage Order*, the FCC does assert in passing that it has a broad mandate to carry out the policies articulated in § 230, see 19 FCC Rcd at 22446 ¶ 35, but that assertion is not essential to the Order. For the reasons explained in this section, we respectfully believe that assertion was incorrect and would not withstand judicial review.

[43] *See* NPRM ¶ 84.

[44] 47 U.S.C. § 1302(a).

[45] It is unclear that § 706(a) grants any authority to the Commission. The primary regulatory responsibility delegated to the Commission in this section is the obligation to produce a report to Congress on whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely manner. *See* 47 U.S.C. § 1302(b). If the report's finding is negative, the Commission is then directed to take action. *Id.* Subsection (a) may simply provide the context for these more specific instructions to the Commission.

[46] *See* 47 U.S.C. § 201(b) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act.").

3. The Commission must focus on transmission facilities.

The FCC's assertion of authority with respect to this rulemaking will be on its most certain legal footing only if the Commission takes a cautious approach to asserting its ancillary jurisdiction. The Commission's jurisdiction is at its strongest if it focuses on *transmission facilities.*[47]

a. Regulatory authority centers on the actual transmission of communications by wire or radio

Regulations relating to the actual transmission of communications by wire or radio are at the core of the FCC's subject matter jurisdiction.[48] Court decisions recognize that the FCC has some authority over "communication[s] by wire or radio," even if an activity or form of communication is not specifically regulated by the Communications Act. To analyze whether the Commission has authority to exercise its ancillary jurisdiction, courts have adopted a two-pronged test. Under this test, authority exists when (1) "the subject of the regulation [is] covered by the Commission's general grant of jurisdiction under Title I," and (2) "the subject of the regulation [is] 'reasonably ancillary to the effective performance of the Commission's various responsibilities.'"[49] Thus, in *United States v. Southwestern Cable Co.*, the seminal ancillary jurisdiction case, the Supreme Court upheld FCC cable regulation under Section 2(a) because it was "reasonably ancillary to the effective performance of the Commission's various responsibilities for the regulation of television broadcasting."[50]

The basis for the Commission to exercise its limited ancillary jurisdiction is the transmission of communications by wire or radio. When the FCC has attempted to regulate activities beyond the transmission of communications by wire or radio, it has typically been found to exceed the established limits of its ancillary jurisdiction. Courts have followed a cautious approach in deciding whether the Commission has validly invoked its ancillary jurisdiction.[51]

---

[47] The NPRM hints at such a focus in characterizing the assertion of authority as extending to "facilities-based" broadband Internet access providers. NPRM ¶ 83; *see also id.* ¶ 84 (referring to "ancillary authority over *facilities-based* Internet access") (emphasis added). But the statutory provisions on which the Commission relies do not on their face contain such a limitation, and the NPRM does not clearly state that the Commission's exercise of authority is (and indeed must be) so confined.

[48] *See* 47 U.S.C. § 151 (2000) (creating the Commission "[f]or the purpose of regulating interstate . . . commerce in communication by wire and radio . . . ."). *See also* 47 U.S.C. § 152(a) ("interstate . . . communication by wire or radio" falls squarely within Congress's grant of jurisdiction to the Commission).

[49] Am. Library Ass'n v. FCC, 406 F.3d 689, 692-93 (D.C. Cir. 2005) (quoting United States v. Sw. Cable Co., 392 U.S. 157, 178 (1968)).

[50] *United States v. Sw. Cable Co.*, 392 U.S. 157, 178 (1968).

[51] *See Am. Library Ass'n*, 406 F.3d at 702 (describing the caution courts have exercised when invoking the Commission's ancillary jurisdiction). *See, e.g.*, FCC v. Midwest Video Corp. (*Midwest Video II*), 440 U.S. 689, 706 (1979) ("Though afforded wide latitude in its supervision over communication by wire, the Commission was not delegated unrestrained authority."). In *Midwest Video II*, the Court held that the Commission exceeded the limits of its ancillary authority in promulgating its access rules. *Id.* at 708. *See also* Motion Picture Ass'n of Am. v. FCC, 309 F.3d 796, 798 (D.C. Cir. 2002) ("Contrary to the FCC's arguments suggesting otherwise, § 151 does not give the FCC unlimited authority to act as it sees fit with respect to all aspects of television transmissions, without regard to the scope of the proposed regulations."). The D.C. Circuit denied the FCC authority under Title I to regulate broadcasting content through its video description rules. *Id.* at 799. "Both the terms of § 1and the case law amplifying it focus on the FCC's power to promote the accessibility and universality of transmission, not to regulate program content." *Id.* at 804.

For example, in *American Library Association v. FCC*, the D.C. Circuit concluded that the FCC could not regulate an activity that occurs after a transmission has been completed. The case involved the FCC's "broadcast flag" regulations, which affected the functionality of receiving devices only *after* a broadcast transmission is complete, and it effectively illustrates when the Commission has exceeded the limits of its ancillary authority.[52] The D.C. Circuit said:

> The Commission's general jurisdictional grant under Title I plainly encompasses the regulation of apparatus that can receive television broadcast content, but only while those apparatus are engaged in the process of receiving a television broadcast. Title I does not authorize the Commission to regulate receiver apparatus after a transmission is complete . . . There is no statutory foundation for the broadcast flag rules, and consequently the rules are ancillary to nothing.[53]

What was critical in that case was that the "broadcast flag" rules attempted to regulate consumer electronic products with regard to functionality *unrelated to* the process of radio or wire transmission. The D.C. Circuit understood that there must be meaningful limits on the scope of the FCC's general jurisdictional grant under Title I and thus rejected the FCC's overreach in that case.[54]

Similarly, *Illinois Citizens Committee for Broadcasting v. FCC* further confirms that FCC regulatory authority centers on the actual transmission of communications by wire or radio. In that case, a complaint to the FCC challenged the impact that the Sears Tower construction would have on television reception in the Chicago area. The Commission denied the requested relief on the grounds that it lacked jurisdiction and the Seventh Circuit upheld its decision. In order for the Commission to exercise its ancillary jurisdiction, both the FCC and the court concluded, an activity must have a closer connection to the actual transmission of communications. The court wrote:

> While the FCC has important responsibilities to promote effective radio and television transmission throughout the country, and thus to minimize interference with radio and television signals, its [ancillary] authority is limited to situations in which the interference is created by, to use the Commission's words, 'a signal-generating' or 'signal-producing' facility. Sections 152 and 153 refer only to transmission facilities.[55]

The case law indicates that FCC authority in this rulemaking proceeding must focus on the actual transmission of communications by wire or radio. Moreover, any data processing performed at an Internet endpoint before or after a transmission of a communication would not be subject to FCC authority because it is beyond the scope of the FCC's general jurisdictional grant of authority under Title I. Thus, the actions of websites and other services on the Internet (such as search engines, social networks, and other sites) would be beyond any arguable authority of the FCC.

---

[52] *Am. Library Ass'n*, 406 F.3d at 691.
[53] *Id.* at 691-92.
[54] "In sum, we hold that, at most, the Commission only has general authority under Title I to regulate apparatus used for the receipt of radio or wire communication while those apparatus are engaged in communication." *Id.* at 704.
[55] *Ill. Citizens Comm. for Broad. v. FCC*, 467 F.2d 1397, 1401 (7th Cir. 1972).

b. The Commission can rarely regulate non-transmission services

In the limited situations when the FCC has been permitted to regulate non-transmission services, there has typically been a risk that entities controlling transmission functions could try to leverage that control to hold up providers of non-transmission services or to otherwise exert improper influence in the market for non-transmission functions. Thus, such regulation targets entities that provide both transmission and non-transmission functions. The FCC has not generally regulated the provision of non-transmission functions by entities with no control over transmission facilities.

For example, in *Brand X*, the Supreme Court upheld classifying cable modem services as "information services," while noting that regulation of information-service providers was nevertheless possible under the Commission's Title I authority.[56] Crucially, the service providers at issue in the case were facilities-based cable companies: "the Commission remains free to impose special regulatory duties on *facilities-based* ISPs under its Title I ancillary jurisdiction."[57] The Court was in no way addressing the FCC's authority to regulate entities that do not control communications transmission facilities.

The same is true in the Commission's *Computer II* proceedings. In affirming the Commission's jurisdiction to enact the *Computer II* rules, the D.C. Circuit was particularly deferential to the Commission's exercise of its ancillary jurisdiction to prevent potential anti-competitive conduct by facilities providers.[58] The FCC hoped to encourage the growth of long distance data processing applications by shielding enhanced services – the functional equivalent of information services today – from common carrier regulation under Title II.[59] However, the Commission was concerned that certain telephone companies could leverage their dominance in the market for last mile transmission services to preclude robust competition in the adjacent market for enhanced services. Thus, the Commission exercised its ancillary authority to regulate the provision of Title I enhanced services by Title II telecommunications carriers. More specifically, the FCC authorized telephone companies to enter the market for enhanced services subject to unbundling and, in certain circumstances, structural separation requirements.[60] These requirements were intended to prevent the telephone company from discriminating in favor of its own enhanced service offerings. The Commission's assertion of ancillary jurisdiction in the *Computer II* proceedings thus provides a useful analogy to the Commission's efforts in this proceeding to ensure providers of broadband Internet access do not leverage their control of transmission services to the detriment of consumers and the Internet generally.

It is a rare exception when the FCC regulates entities that do not control transmission facilities, such as certain VoIP providers.[61] This occurs only when a service threatens a very specific and

---

[56] *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).
[57] *Id.* at 996.
[58] *Computer & Commc'ns Indus. Ass'n v. FCC*, 693 F.2d 198 (D.C. Cir. 1982) (although the Commission did not impose Title II regulation on enhanced services or customer premises equipment, the D.C. Circuit agreed that it has ancillary jurisdiction over both under Sections 152 and 153).
[59] *Id.* at 205-06.
[60] *Id.* Under the structural separation requirement, the largest telephone companies could provide enhanced services only through a formally separate subsidiary.
[61] "While Congress has indicated that information services are not subject to the type of regulation inherent in Title II, Congress has provided the Commission with ancillary authority under Title I to impose such regulations as may be necessary to carry out its mandates under the Act. Although the Commission has clear authority to do so, it has only

non-competition-related task that has been explicitly assigned to the FCC. For example, in the FCC's VoIP E911 Order, the Commission imposed E911 requirements on interconnected VoIP providers under its Title I ancillary authority in order to ensure an effective 911 system.[62] There, the Commission relied on Title I, Section 1's reference to "promoting safety of life and property through the use of wire and radio communication" as a basis for ancillary jurisdiction.[63] Similarly, the FCC regulated entities that do not control transmission facilities in its 1999 Section 255 Order.[64] There, the Commission asserted ancillary jurisdiction to extend the disability access requirements of Section 255 to the providers of voicemail and interactive menu service. However, the Commission's assertion of ancillary jurisdiction over these two information services was specifically discrete and limited:

> Unlike voicemail and interactive menus, other information services discussed by commenters do not have the potential to render telecommunications services themselves inaccessible. Therefore, we decline to exercise our ancillary jurisdiction over those additional services.[65]

The FCC should be particularly careful not to overreach and misuse its very limited authority over non-transmission services in this proceeding, nor to assert a jurisdictional basis that could encourage such misuse in future proceedings.

B. Recommendations for a narrow and focused basis for jurisdiction

1. Ancillary jurisdiction under Title I

CDT urges the FCC to rely on Title I of the Communications Act as an independent source of authority that supports a limited basis for ancillary jurisdiction in this rulemaking. Any such claim of jurisdiction must be expressly limited to the authority to prevent interference with Internet *access,* and must disavow any general regulatory authority over the Internet, specifically authority that might extend to the content of communication on the Internet or the behavior of any entity that does not provide actual transmission capabilities. Although its language is general, Title I does not imply that the Commission's ancillary jurisdiction is unlimited or unconstrained, and it plainly would be subject to the limits on FCC action – including limits on content regulation – discussed above.[66]

Relevant case law establishes that Title I alone can provide the Commission with the necessary regulatory authority to exercise ancillary jurisdiction in this proceeding, so long as the rules are

---

rarely sought to regulate information services [such as VoIP] using its Title I ancillary authority." *Vonage Holdings Corp.*, 19 FCC Rcd 22404, 22426 (2004).

[62] *IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers*, 20 FCC Rcd 10245 (2005) [hereinafter "VoIP E911 Order"].

[63] *Id.* at 10262.

[64] *Implementation of Sections 255 and 251(a)(2) of the Communications Act of 1934, as Enacted by the Telecommunications Act of 1996: Access to Telecommunications Service, Telecommunications Equipment and Customer Premises Equipment by Persons with Disabilities*, 16 FCC Rcd 6417 (1999) [hereinafter "Section 255 Order"].

[65] *Id.* at 6461.

[66] *See supra* Part III.A. "Under § 1, Congress delegated authority to the FCC to expand radio and wire transmissions, so that they would be available to all U.S. citizens. Section 1 does not address the *content* of the programs with respect to which accessibility is to be ensured. In other words, the FCC's authority under § 1 is broad, but not without limits." *Motion Picture Ass'n of Am. v. FCC*, 309 F.3d 796, 804 (D.C. Cir. 2002).

defined to address particular conduct that unreasonably impedes open and unfettered access to the broadband Internet.[67] First, the subject of the regulation at issue here is covered by the Commission's general grant of jurisdiction under Title I. That is, the regulation relates to the actual transmission of communications by wire or radio controlled by entities that provide subscribers with connections to the Internet.[68] And second, preserving the open Internet is "reasonably ancillary" to the effective performance of the Commission's various responsibilities under the Title I provisions. The Title I provisions specifically call on the FCC to assure a "rapid, efficient" nationwide system of wire and radio communications services.[69] Given the proven success of the Internet's open communications architecture, it should be apparent that protecting the network's open character directly serves the goal of ensuring a modern and efficient nationwide communications system. A less open Internet simply would not be as efficient, effective, and universally accessible as a platform for independent communications.[70]

This type of analysis under the two-pronged ancillary jurisdiction test is directly supported by the cases. Prior court decisions have upheld FCC regulations "reasonably ancillary" to responsibilities that come directly from the language of Title I alone – these cases do not cite any other source of authority outside Title I to justify the Commission's exercise of its ancillary jurisdiction.[71] In addition, in *Brand X* the Supreme Court explicitly suggested that while facilities-based providers of broadband Internet access, such as cable modem services, were not subject to mandatory common-carrier regulation under Title II, "the Commission has jurisdiction to impose additional regulatory obligations under its Title I ancillary jurisdiction to regulate interstate and foreign communications."[72] The Court concluded that "the Commission remains free to impose special regulatory duties on facilities-based ISPs under its Title I ancillary jurisdiction."[73]

Thus, while facilities-based Internet service providers may not at this time be treated as Title II common carriers, Title III spectrum licensees, or Title VI cable operators, relevant case law and sound public policy suggest that the FCC still has limited ancillary jurisdiction over these entities

---

[67] *See, e.g.*, United States v. Sw. Cable Co., 392 U.S. 157, 171-72 (1968) (specifically holding that Title I could also provide regulatory authority, not merely subject matter jurisdiction, independently of other provisions); United States v. Midwest Video Corp., 406 U.S. 649, 660 (1972) ("We also held [in *Southwestern Cable*] that § 2(a) is itself a grant of regulatory power"); Gen. Tel. Co. of the Sw. v. United States, 449 F.2d 846, 853 (5th Cir. 1971) ("The Supreme Court . . . has concluded that Section 2(a) of the Communications Act alone is sufficient to support the Commission's assertion of jurisdiction over CATV systems."); Computer & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198, 213 (D.C. Cir. 1982) ("[I]t [is] settled beyond peradventure that the Commission may assert jurisdiction under section 152(a) of the Act over activities that are not within the reach of Title II . . . One of [the Commission's various responsibilities] is to assure a nationwide system of wire communications services at reasonable prices."); Rural Tel. Coal. v. FCC, 838 F.2d 1307, 1315 (D.C. Cir. 1988) (citing Sections 151 and 154(i) as the statutory basis for exercising ancillary jurisdiction to uphold the creation of the universal service fund); GTE Serv. Corp. v. FCC, 474 F.2d 724, 730-31 (2d Cir. 1973) (citing the Commission's responsibility to ensure efficient and economic service to the public under Sections 151 and 154(i) as a statutory basis for exercising ancillary jurisdiction).

[68] *See* 47 U.S.C. § 151 ("commerce in communication by wire and radio").

[69] *Id.*

[70] In addition, less open systems in which network operators charge for special priority can create perverse incentives regarding bandwidth scarcity, making this proceeding relevant to the speed of the communications system as well. *See infra* Part V.C.

[71] *See Rural Tel. Coal.*, 838 F.2d at 1315 (citing responsibility to promote "reasonable charges"); *Computer & Commc'ns Indus. Ass'n*, 693 F.2d at 213 (citing responsibility to promote "reasonable prices"); *NARUC v. FCC*, 880 F.2d 422, 429-30 (D.C. Cir. 1989) (citing § 151 as "goals of the Act" that can be implemented "with respect to interstate communication").

[72] *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 976 (2005).

[73] *Id.* at 996.

under Title I to address actions by facilities-based providers that could impede users' access to the Internet. In asserting such jurisdiction, however, the Commission should expressly state its understanding that such authority does not and could not extend beyond the provision of actual transmission services to Internet matters more generally.

2. Alternatively, reclassification of broadband Internet access service as a telecommunications service under Title II

Although it would require careful consideration and a Further NPRM, the Commission could establish clear jurisdiction if it were to return broadband Internet access service to be regulated as a telecommunications service under Title II. As the Supreme Court has plainly said the FCC can do,[74] the Commission could "change course" and bring Internet access back under Title II, while at the same time forbearing from rate regulation and other unneeded aspects of that regime. Such an approach would provide ample – but appropriately focused – authority for the FCC to issue its proposed neutrality rules.

IV. Codifying the Existing Four Internet Principles

CDT agrees that codifying the four existing principles will protect innovation and online free expression, including civic participation and democratic engagement. The policies the principles express are essential to an Internet that allows full participation and innovation without the permission of gatekeepers. Codifying the principles into rules will strengthen the Commission's commitment these policies and remove uncertainty as to their enforcement.

The Commission is right to frame the proposed rules as obligations on broadband Internet *access* providers.[75] Indeed, as argued immediately above, sound policy and legal considerations demand a narrow focus on transmission facilities. As a practical matter, these facilities present the most likely bottlenecks that could be used to effectively limit consumer choice among content, applications, services, and devices. CDT also agrees that dial-up access should be excluded. There is no need to place additional regulations on access over facilities that are already covered under Title II common carriage rules.

The NPRM specifically asks for comment on one commenter's suggestion that openness rules should apply to content, application, and service providers in addition to broadband access providers.[76] This suggestion should be expressly dismissed. As argued above, extending the rules to these entities would reach beyond the Commission's authority and would likely be unconstitutional. Doing so would also contravene the policy goals of the rulemaking. As the NPRM recognizes, the Internet's open transmission architecture fosters speech and innovation.[77] By contrast, regulating what lawful applications and services can and cannot do when employing that architecture would make the Internet a *less* open platform than it is today.

CDT also supports the Commission's proposed change from "accessing" content to "sending and receiving . . . content."[78] The ability for all users to send as well as receive information is a

[74] *See id.* at 1001.
[75] NPRM ¶ 90 (emphasis added).
[76] *Id.* ¶ 101.
[77] *Id.* ¶ 62.
[78] *Id.* app. A, Proposed Rules § 8.5; *Id.* ¶ 95.

critical factor in the Internet's unprecedented empowerment of speech, participation, and engagement. CDT notes that this change will mean that prohibitions on operating servers over residential broadband connections will be impermissible. Such prohibitions in carrier "terms of service" are common today,[79] but they are inappropriate legacies from a time when the vast majority of residential traffic was in the downstream direction only. Now, a broad range of consumer-focused applications – such as Skype and BitTorrent – operate as servers in the residential context, meaning that they send traffic in the upstream direction at the request of other computers. There is no reason that innovation in new applications using home servers should be prohibited.[80] Disallowing such use-specific restrictions is precisely the function of the FCC's proposed rules and is in line with the goal of ensuring that Internet users are able to employ their Internet connections as they see fit, rather than as broadband Internet access providers choose to allow. As discussed below with respect to reasonable network management, providers should remain free to manage upstream congestion through evenly-applied volume-based policies, but singling out and prohibiting what could be quite low-volume servers is not reasonable network management.[81]

V. Codifying a Principle of Nondiscrimination

CDT strongly agrees that a nondiscrimination principle is an essential component of a framework to protect the Internet's open nature. CDT believes, however, that the proposed rule and its accompanying explanation at paragraph 106 should be modified to provide better guidance and reduce the risk of discouraging benign conduct. In addition, the Commission should clearly describe at least two specific kinds of differential treatment – routing policies that differentiate based on subscribers' individual bandwidth usage volumes or as directed by the subscribers themselves – that will not be considered "discriminatory" within the meaning of this rule.

A. Clarifying the definition and explanation of "nondiscrimination"

1. Concerns with the NPRM's formulation

CDT has two concerns with the NPRM's formulation of a nondiscrimination principle.

First, the NPRM explains the nondiscrimination rule as meaning that "a broadband Internet access service provider may not *charge* a content, application, or service provider" for special treatment.[82] While charging for favorable treatment is certainly a possibility that the nondiscrimination rule should address, it is not the only scenario in which potentially harmful

---

[79] *See, e.g.*, Verizon Online Terms of Service, http://www.verizon.net/policies/vzcom/tos_popup.asp (last visited Jan. 14, 2010); Comcast Acceptable Use Policy for High-Speed Internet Services, http://www.comcast.net/terms/use/ (last visited Jan. 14, 2010); Time Warner Cable Residential Services Subscriber Agreement, http://help.twcable.com/html/twc_sub_agreement.html (last visited Jan. 14, 2010).

[80] Indeed, some privacy advocates have suggesting designing servers for the home that can store a user's private information, and serve it over the public Internet only to those authorized to receive the information. But this home "privacy server" idea could not be deployed in an environment in which servers are prohibited in the home.

[81] *Cf. Comcast Opinion and Order* ¶ 51 (holding that Comcast's practice of selectively blocking even high-volume BitTorrent uploads posed "a substantial threat to both the open character and efficient operation of the Internet, and [was] not reasonable."). It would be ironic for the Commission to protect high-volume upstream BitTorrent usage but not protect lower-volume upstream server usage.

[82] NPRM ¶ 106 (emphasis added).

discrimination could occur. A broadband Internet access service provider could elect to discriminate for reasons other than direct payment. It could provide favorable treatment to its own, proprietary content and services; to the content and services of entities that agree to partner with it in some other aspect of its business; or to other selected content, services or applications for virtually any competitive, strategic, or even viewpoint-related motivation. A meaningful nondiscrimination rule should not be limited to the paid priority scenario. In short, the rule should cover the *provision* of special treatment, not just the *charging for* special treatment.

Second, the NPRM says that the nondiscrimination rule applies to the provision of "enhanced or prioritized access to the subscribers."[83] This formulation is in one respect too narrow and in one respect too broad.

It is too narrow because while discrimination could take the form of enhancing or prioritizing selected traffic, it could also take the form of degrading or decreasing the priority of selected traffic. The nondiscrimination rule should apply to either scenario.

The formulation is too broad because not every type of "enhanced access to subscribers" poses a risk to the Internet's openness. For example, a broadband Internet access service provider might offer caching, which enables content providers to store commonly requested content on servers that are closer to intended recipients. The end result is enhanced delivery to subscribers. Similarly, a broadband provider might allow large content providers to interconnect with its network at convenient points, again with the goal of delivering the content more quickly and efficiently to subscribers.

In both cases, delivery of content is "enhanced" by activities (storing data on a server, interconnecting with someone else's facilities) that occur at the boundary of the broadband provider's network. There is no enhanced or prioritized treatment in the actual *transmission* of packets across the broadband provider's network. And since no packets are given priority over other packets at the router level, these techniques should not negatively impact other, non-prioritized traffic. In contrast, when selected packets are permitted to "cut in line" in router queues, prioritizing selected traffic necessarily entails decreased priority for the non-favored traffic.

As an analogy, consider a municipal road system. A company seeking to speed its deliveries to customers could try to convince city officials to give its delivery trucks priority on the roads – say, allowing the trucks to cut in front of other vehicles at congested intersections and red lights. This would be akin to router-level discrimination in a broadband network; the trucks would have special priority on the transmission links (roads) that carry traffic across the network.

As a completely different approach, the company could build delivery hubs at a number of locations around the city. Deliveries to customers would be enhanced by shorter drive times, even as the flow of traffic over the roads remained nondiscriminatory. This would be akin to caching or interconnection: Delivery is enhanced not by playing favorites in the carriage of traffic across the network's transmission links, but rather by activities at the network's edge.

CDT believes the nondiscrimination principle should focus expressly and exclusively on discrimination in the interior of a broadband provider's network – that is, on discrimination at the

[83] *Id.*

level of the routers that control transmission. Activities that occur at the boundary of the network, such as caching and interconnection, should not fall within the scope of the rule.[84]

2. Recommendation for a revised nondiscrimination rule

It should not be difficult to formulate a nondiscrimination rule that avoids the concerns raised above. CDT recommends revising the nondiscrimination rule to read as follows:

Subject to reasonable network management, a provider of broadband Internet access service must route and transmit lawful communications across its network in a manner that is nondiscriminatory with respect to content, source, destination, ownership, application or service.

Note that this formulation adds source, destination, and ownership to the list of impermissible bases for discrimination; the NPRM's proposed rule cites only content, applications, and services. Adding the three additional terms safeguards against the possibility that discrimination could target all communications with or owned by a particular entity regardless of the content, application, or service. It also is consistent with the "Net Neutrality" commitments made by AT&T in connection with the Commission's approval its merger with BellSouth.[85]

Importantly, this formulation of the principle (a) does not depend upon whether discrimination is motivated by direct payment; (b) is not limited to any particular form of discrimination (enhancing versus degrading); and (c) focuses exclusively on the routing of communications across the broadband provider's network.

B. Identifying specific behaviors that will *not* be considered discriminatory

As the NPRM notes, it would be helpful to identify and describe some *ex ante* exceptions to the general nondiscrimination rule.[86]

1. Treatment based on service plans and bandwidth usage patterns

The NPRM proposes that a nondiscrimination rule "would not prevent a broadband Internet access service provider from charging subscribers different prices for different services."[87] This is an important exception, and the Commission should spell out more clearly what it means. Specifically, providers of broadband Internet access service should be free to devise subscription plans that charge individual subscribers different amounts based on such factors as speed or usage volume (i.e., the amount of data actually sent or received). So long as the prices

---

[84] This is not to say that discrimination in the offering of caching or interconnection could never pose concerns. For example, if a provider of broadband Internet access service were to offer caching on an exclusive or limited basis while also stifling independent caching providers like Akamai by denying them the interconnection they need to operate, the competitive implications could be significant. Today, however, independent third-party caching is widely available. Moreover, the focus of this rulemaking should be on preserving the Internet's open and transparent transmission architecture, not on foreclosing each and every theoretical way that a provider of broadband Internet access service could attempt to impair online competition. Actions at the edge of the network, even if their effects may be anticompetitive, are simply outside the proper scope of this rulemaking.

[85] *AT&T, Inc. and BellSouth Corp., Application for Transfer Control*, FCC 06-189, app. F at 154 (2007) (committing AT&T/BellSouth for two years to refrain from providing any service that privileges, degrades, or prioritizes Internet traffic "based on its source, ownership, or destination"), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-189A1.pdf.

[86] NPRM ¶ 110.

[87] *Id.* ¶ 106.

and terms focus on *how much* Internet capacity a subscriber gets or uses (and perhaps *when* he or she gets or uses it[88]) – rather than *what he or she uses it for* – the plan does not favor particular content, applications, or services over others.[89]

Nor would actions taken to enforce the terms of such service plan offerings constitute discrimination. A provider of broadband Internet access service might differentiate between packets bound for a subscriber who has exceeded a specified usage cap and packets bound for subscribers who have not. Such actions, taken to implement generally applicable policies and limitations tied to the service offerings that different subscribers have purchased, should not run afoul of the nondiscrimination rule.

Indeed, treating packets differently based on the bandwidth usage patterns of the individual subscribers sending or receiving them should not violate the nondiscrimination rule even when usage limits are not directly tied to differences between service plans. For example, a broadband provider could have a general policy of responding to congestion by rate-limiting the traffic of individual subscribers who are contributing the most to the congestion. So long as such a policy is suitably transparent, enforcing it should not subject the broadband provider to claims of discriminating against the rate-limited subscribers.

The key, of course, is that usage-based policies and actions should not hinge in any way on the content or application of subscribers' Internet communications or the identities of the parties with whom the subscribers are communicating. This is what makes them nondiscriminatory. The provider of broadband Internet access service focuses only on the identity and usage volumes of its own subscribers, and does not differentiate or play favorites between providers of Internet content, applications, or services.

2. Prioritizing traffic as directed by subscribers

The Commission should also state clearly that the nondiscrimination rule will not prohibit providers of broadband Internet access service from enabling *individual subscribers* to designate how their different inbound or outbound traffic streams should be prioritized.

The fundamental justification for a nondiscrimination rule is that having *broadband providers* actively determine which content, applications, or services will get favorable (or unfavorable) treatment poses significant risks to the Internet's open nature. It could enable broadband providers to steer subscriber choices, by making some content, applications or services work more smoothly than others. This in turn could create pressure for providers of content, applications, or services to negotiate with broadband providers to ensure favorable treatment. In short, the ability to select traffic for priority could give broadband providers significant gatekeeping leverage.

[88] For example, a service plan could distinguish between peak and non-peak congestion times – say, imposing limits or surcharges on a subscriber's bandwidth usage during peak congestion hours or giving a subscriber a "bandwidth boost" that speed data transfer during non-peak hours.

[89] Certain service plan terms could have the practical effect of favoring applications or services that use less bandwidth over those that use more; a cap on weekly or monthly bandwidth usage, for example, could make subscribers reluctant to use more bandwidth-intensive applications. This is entirely different, however, from the broadband provider exercising discretion to pick and choose which particular applications to favor and which not.

In contrast, putting *subscribers* in control of priority designations that are truly "portable" – i.e., that may be applied to whatever content, applications or services each subscriber may choose (so that one user might choose to prioritize a VoIP application, while another user might choose to prioritize a gaming application) – does not pose the same risks. The broadband provider does not get any particular leverage, because the ability to select which traffic gets priority lies with individual subscribers. Meanwhile, an entity providing content, applications, or services does not need to worry about striking up relationships with various broadband providers to obtain top treatment. All it needs to worry about is building relationships with users and explaining to those users whether and how they may want to select the particular content, application, or service for priority treatment.

The Commission need not involve itself in the all the practical details of how subscriber-selected prioritization might be implemented; that is a matter for providers of broadband Internet access service to resolve. But there is no reason to suggest that this kind of subscriber-driven approach could not work. From a technical perspective, existing standards, such as the DiffServ architecture standardized by the IETF, provide ways for assigning priority levels to different traffic.[90] On the non-technical side, it would be important to create incentives for subscribers to assign priority appropriately based on the real performance needs of their different applications, rather than just trying to mark all their traffic as high priority. This too has been a topic of discussion at IETF, and one can imagine a variety of possible approaches.

For example, a broadband provider might offer subscription plans that allow a certain volume of high, medium, and low priority usage each month – in effect, discrete "buckets of bits" that encourage users to deploy high priority only when doing so is truly useful. Or subscribers could get some kind of bandwidth "boost" if they mark their non-latency-sensitive traffic as low priority. Pricing incentives are obviously possible as well.

A subscriber-driven prioritization system need not be excessively complicated either. Providers of broadband Internet access service could create some default settings that work well for most subscribers, but can be easily changed by subscribers who want to prioritize new or obscure content, applications or services. Applications providers that believe their products would benefit from prioritization could explain to users, in connection with the installation process or otherwise, how to designate appropriate priority.[91]

C. Impact of requiring nondiscrimination

The NPRM asks a number of questions regarding the likely impact of a nondiscrimination requirement.

Paragraph 111 asks about the effect on social welfare and future innovation. CDT believes that a nondiscrimination rule will promote both. The innovations fostered by the Internet have generated a huge amount of economic value. Major companies, entirely new categories of products and services, and e-commerce of many kinds have arisen virtually from scratch. Greater competition has been introduced into many markets as Internet-based endeavors

[90] Steven Blake et al., *An Architecture for Differentiated Services*, IETF RFC 2475 (1998), http://www.ietf.org/rfc/rfc2475.txt.

[91] Nothing in the rules would prohibit a broadband provider from charging subscribers a fee for the ability to designate traffic for prioritization. Nor would the rules prevent an application provider – interfacing directly with its users, rather than with the broadband provider – from offering users some kind of rebate to offset the cost.

challenge traditional business models. Tremendous non-economic value has been created as well. Bloggers and user-generated content sites like YouTube have enabled broader participation in civic and political discourse, and endeavors like Wikipedia are showing the potential of Internet-based collaboration outside the commercial realm.

These benefits are directly tied to the Internet's complete absence of barriers to entry for independent speakers and innovators. Discrimination could undermine this key trait, creating new barriers to independent speech and innovation by making permission, approval, or at least acquiescence of broadband providers a prerequisite for online success. A nondiscrimination rule can safeguard the Internet's ability to provide a platform where speech and innovation can prosper with complete independence from network operators. This creates social value. The network's nondiscriminatory character creates major spillover benefits to the economy and to society.

Paragraph 112 asks about the impact of a nondiscrimination rule on Internet users. First and foremost, users will continue to enjoy the fruits of innovation that grow from the open structure a nondiscrimination rule protects. Moreover, the type of nondiscrimination rule described above would not create any disadvantage for users. The rule would not prohibit caching, which is widely used today to speed delivery of content to Internet users. Providers of broadband Internet access, barred from prioritizing traffic at their own discretion, might well decide to deploy the kind of user-driven prioritization described in section B.2. above – a result that would give users a welcome degree of flexibility and control without carrying risks to innovation.

The Commission should be very skeptical about claims that a nondiscrimination rule would harm end users by undermining the quality or utility of particular content, applications, or services.[92] First, providers of many applications and services such as VoIP have found ways to meet latency challenges and roll out successful products without any kind of router-level priority. The Internet is sufficiently robust to handle the vast majority of functions.

Second, even if prioritization were to prove crucial in some cases, the nondiscrimination rule suggested here offers at least two options for meeting that need. Allowing subscribers to designate applications for prioritized treatment would be permitted, as discussed above. Providers of broadband Internet access could facilitate the delivery of particularly sensitive services by enabling subscribers to specify priority as needed, rather than deciding on a centralized basis which applications will get the benefit of priority. Alternatively, as discussed below, broadband providers could choose to offer certain content, applications or services as managed or specialized services. CDT agrees with the Commission's suggestion that services receiving special transmission treatment by the provider of broadband Internet access service should "be more properly understood as managed or specialized services rather than as broadband Internet access services."[93]

The NPRM also asks about the likely impact on network deployment.[94] CDT believes a nondiscrimination rule may play an important role in preserving the network deployment incentives of providers of broadband Internet access service. Specifically, if providers came to depend upon prioritization fees from non-subscribers for a significant portion of their revenue,

[92] *See* NPRM ¶ 113.
[93] *Id.*
[94] *Id.*

that would give them a financial interest in bandwidth *scarcity* – because in the absence of scarcity and the resulting congestion, nobody would need to purchase priority. From the network operator's perspective, investments to expand network capacity would carry the risk of decreasing revenues from prioritization revenues. This perverse incentive can be avoided through a nondiscrimination rule.

D. Prioritizing classes of services

The NPRM asks about the practical consequences of allowing providers of broadband Internet access to "manage their networks to assure quality of service to particular types of traffic – e.g., all VoIP traffic."[95]

As a preliminary matter, differentiating based on traffic type would certainly constitute discrimination; traffic is treated differently based on the application or service with which it is associated. Within the structure of the Commission's rules, the only question should be whether such discrimination qualifies as "reasonable network management."

Discriminating based on traffic type does not give a provider of broadband Internet access service as much leverage and control as discriminating for or against individual content, applications, or services. The broadband provider does not get to select individual favorites, nor make financial deals that create perverse incentives for scarcity.

Nonetheless, CDT believes that providers of broadband Internet access should not be permitted to discriminate based on traffic class. Allowing such discrimination begs the question of who gets to make classification decisions. The Internet is constantly seeing the rise of new and innovative applications, and it often will not be obvious how new applications should be classified. If broadband providers have discretion to determine how novel or hybrid applications will be classified, and thus what level of priority they will receive, those providers may exercise substantial leverage over which applications will succeed or fail. An innovator with a new application, instead of focusing exclusively on recruiting end users, may need to consider contacting providers of broadband Internet access to lobby for favorable classifications.

There is also a risk that a broadband provider's classification choices could be tinged by competitive considerations. Faced with an application for which the appropriate classification is debatable, a broadband provider could be tempted to choose the class that gets the lower priority if the application competes with one of the provider's own products.

Moreover, prioritizing based on traffic type would require broadband Internet access providers to actually know the traffic types of the numerous packets flowing over their networks. This would require extensive monitoring, which carries major privacy implications. Efforts to identify traffic based on a simple characteristic such as port number would likely be thwarted quickly, with many applications changing port numbers or taking other steps to appear to be whatever class of traffic receives favorable treatment.

If the Commission chooses to permit prioritization based on traffic class at all, it should at a minimum require that traffic from unknown applications – perhaps new, or perhaps niche applications that the broadband provider simply has not encountered yet – should be treated as

[95] *Id.*

belonging to the most favorable traffic class. Having a default rule of high priority could reduce the risk that new applications that would benefit from priority will feel compelled, as a prerequisite to rollout, to convince broadband providers to put them on the list of the favored application class. In addition, the Commission could consider whether any independent standards body might be in a position to make classification decisions, rather than leaving each provider of broadband Internet services to make those decisions individually. Both steps could help limit the ability of broadband providers to serve as gatekeepers with leverage over the success or failure of new content, applications, or services.

E. The First Amendment implications of a non-discrimination rule

The NPRM seeks comment on whether a nondiscrimination rule would "promote free speech, civic participation, and democratic engagement," whether discrimination by access providers would harm those goals, and whether any rule imposed by the FCC would interfere with the First Amendment rights of providers of broadband Internet access services.[96]

As Judge Stewart Dalzell wrote in 1996 in concurring in the original trial court decision striking down the Communications Decency Act, the "Internet is a far more speech-enhancing medium than print, the village green, or the mails."[97] Dalzell summarized four speech-enhancing characteristics of the Internet:

> First, the Internet presents very low barriers to entry. Second, these barriers to entry are identical for both speakers and listeners. Third, as a result of these low barriers, astoundingly diverse content is available on the Internet. Fourth, the Internet provides significant access to all who wish to speak in the medium, and even creates a relative parity among speakers.[98]

In considering the CDA that was before the court, Judge Dalzell sought to avoid "an Internet that mirrors broadcasting and print, where economic power has become relatively coterminous with influence."[99] It is this open Internet, where both small and large speakers can reach a global audience without prior negotiation or approval, that has made the Internet into the most politically empowering medium to ever exist. The dynamic and diverse political speech that emerged in the 2006 and 2008 U.S. elections is a strong validation of this aspect of Internet speech.

Discrimination by Internet access providers could directly threaten these speech-enhancing characteristics. If broadband providers are able to favor a preferred Internet video provider, then they can favor a preferred news provider, and a preferred political analysis provider. They would be able to move the Internet toward the model of broadcast and cable, in which only those speakers with money and corporate connections have ready and effective access to the national audience. This would gravely threaten the explosion of "free speech, civic participation, and democratic engagement" that the Internet has brought.

---

[96] *Id.* ¶ 116.
[97] *ACLU v. Reno*, 929 F. Supp. 824, 882 (E.D. Pa. 1996) (Dalzell, J., concurring).
[98] *Id.* at 877.
[99] *Id.* at 878-79.

The NPRM asks whether a non-discrimination rule would infringe on the First Amendment rights of broadband providers – an assertion similar to First Amendment claims made by cable companies in the late 1990s in the "open access" debates.[100] This simple answer is "no," for a number of reasons. Most simply, broadband providers are not engaging in their own speech through the provision of Internet access – they are simply communications conduits, and as such they do not have First Amendment objections to a requirement that they carry all communications. Just as a telephone company cannot challenge a common carriage requirement under the Constitution, a broadband provider could not overturn a non-discrimination requirement.[101]

Even if the speech rights of broadband providers were arguably implicated, the standards set out in the *Turner* line of "must carry" cases[102] would not be met. Unlike in those cases – where cable companies were exerting "editorial control" over which channels to carry – broadband providers are offering access to the entire Internet, and a non-discrimination principle would not be a content-based imposition on that offering. Moreover, unlike with cable channels, there is no reasonable possibility that broadband users would be confused to think that their ISPs "approved of" or was otherwise associated with all of the myriad websites available on the Internet (and thus the "compelled speech" arguments made in *Turner* would not be present). In any event, the speech burdens that the Supreme Court *upheld* in *Turner* were constitutionally more burdensome than those presented by a non-discrimination rule, and thus such a rule would be upheld even under the "intermediate scrutiny" approach taken in *Turner*.[103]

VI. Codifying a Principle of Transparency

CDT also strongly supports the Commission's inclusion of a transparency principle among the proposed rules. Disclosure of network management practices will empower consumer choice, improving competition among broadband Internet access service providers, and will enable consumers to make more efficient use of the services they purchase. Additionally, disclosure of network management practices to innovators will help ensure widespread efficient operation of existing applications and services as well as those that have yet to be created.

Disclosure should be sufficiently detailed to be useful for subscribers as well as content, application, and service providers. Critically, this means the transparency rule must not be subject to an exception for reasonable network management. With regard to the level of detail required, as well as the risks that detailed disclosure might pose, CDT proposes that the Commission consider adopting different guidelines for disclosure of congestion management practices and security management practices. Additionally, we note several other aspects of broadband service where transparency will provide important safeguards against practices that

[100] For a thorough analysis of – and debunking of – the constitutional claims asserted in open access cases, see Harold Feld, *Whose Line is it Anyway? The First Amendment and Cable Open Access*, 8 COMMLAW CONSPECTUS 23 (2000).

[101] *See* Jack Balkin, *Free Speech and Press in the Digital Age: The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 430, n.15 (2009).

[102] *See* Turner Broad. Sys. v. FCC (*Turner I*), 512 U.S. 622 (1994); Turner Broad. Sys. v. FCC (*Turner II*), 520 U.S. 180 (1997).

[103] One case from the open access era did decide that open access rules would violate the First Amendment rights of cable operators, *see Comcast Cablevision of Broward County v. Broward County*, 124 F. Supp. 2d 685 (S.D. Fla. 2000), but that decision is based on such fundamental misconceptions about Internet service (and it is in such tension with the *Turner* analysis) that the decision is not persuasive.

could threaten the open Internet. With regard to the methods of disclosure, open, Web-based public disclosure will provide the widest benefit while minimizing the regulatory burden on broadband providers.

A. Removing the exception for reasonable network management

Foremost, to be useful to subscribers and application developers, it is crucial that the transparency rule apply to all network management practices. The Commission has proposed that the transparency rule be subject, like the other rules, to "reasonable network management."[104] The network management exception may be appropriate in the context of the other rules, such as the prohibitions on blocking or discrimination, but it would be counterproductive as applied to the transparency rule.[105]

The proposed definition of reasonable network management includes practices that, however reasonable, could noticeably affect individual user's traffic or the performance of particular applications, and therefore warrant disclosure. For example, if a heavy user experiences traffic throttling as part of an evenly applied, volume-based policy for managing congestion, that policy should be disclosed to avoid consumer confusion and frustration. Disclosure of such policies could also help application developers to design their products to reduce their impact on network congestion.

Exempting reasonable network management from the transparency rule would negate these benefits. Once the Commission finalizes its rules, broadband providers presumably will be careful to avoid *unreasonable* network management practices, since such practices will likely contravene the rules. Therefore, if reasonable practices are exempt from disclosure, the overwhelming majority of network management practices that could actually affect subscribers and applications providers could remain undisclosed. Mandatory transparency would apply only in the unlikely event that a broadband provider engages in practices that it recognizes as being unreasonable. This is an absurd result that would completely undermine the value of transparency to subscribers and other stakeholders.

B. Elements of disclosure

1. Guiding the appropriate level of detail

The NPRM provides a general framework that leaves many details to be fleshed out in future adjudications.[106] This is appropriate for the transparency rule as the details of particular network management practices that merit disclosure will depend on the nature of particular practices, and specifically on the risk of circumvention that disclosure poses. The Commission should nonetheless provide some guiding principles for what will be "reasonably required"[107] under the rule, without being overly prescriptive.

---

[104] NPRM ¶ 119.
[105] The transparency rule should, however, remain subject to the other exceptions identified in the NPRM, which provide for the needs of law enforcement, public safety, and homeland and national security. *Id.* ¶¶ 142-147.
[106] *Id.* ¶¶ 89, 118, 134.
[107] *Id.* app. A, Proposed Rules § 8.15.

While more detail will be appropriate for some practices, the Commission should express the general expectation that, at a minimum, broadband providers should disclose with respect to each particular network management practice:

- what actions are taken;
- what legitimate purpose is served;
- the effect on subscribers' use of the service;
- the criteria that trigger the action; and
- what redress process is available to users wrongfully targeted by the practice.

As the NPRM acknowledges, providing this information will benefit potential and current subscribers, whose use of broadband Internet service and chosen applications may be directly impacted by network management policies.[108] For example, a heavy BitTorrent user shopping for Internet service might be very interested to know which of the broadband providers in his or her local area degrades high-volume subscribers' traffic as a means of controlling congestion. Additionally, knowledge of network management techniques and how and when they apply can be useful to broadband consumers in making efficient use of their bandwidth and understanding and contesting perceived problems with their service.

As the NPRM notes, meaningful disclosure of network management practices will also be valuable to content, application, and service providers.[109] Adhering to known standards and publicly posting management practices will enable innovators to work within the bounds of management policies to ensure that new services work as well as they can – providing maximum consumer benefit and the most efficient use of network resources. Network management disclosure should be sufficiently descriptive to provide these benefits. In particular, disclosure of the techniques used to manage congestion should include technical details to guide users and developers in avoiding congestion in the first place.

2. Risk of circumvention

In CDT's view, two types of network management discussed in the NPRM – practices to reduce or mitigate the effects of congestion (congestion management)[110] and practices to address harmful or unwanted traffic (security management)[111] – will require different levels of detail in their disclosures. This difference largely turns on the risk of circumvention posed by disclosure of these practices, an issue on which the NPRM requests comment.[112] Disclosure of security management practices poses the risk of malicious circumvention; disclosure of congestion management policies largely does not.

Congestion results when the amount of traffic on a shared link exceeds that link's capacity. While certain users may contribute vastly more to a congested link than others by transmitting more traffic, merely transmitting a high volume of bits is not a malicious act. Network operators offer certain bandwidth levels to their customers, and those customers who make extensive use of their connections (within the bounds set by their terms of service) are merely extracting value from the service that they paid for.

---

[108] *Id.* ¶¶ 121-26.
[109] *Id.* ¶ 127.
[110] *Id.* ¶ 135(a)(i).
[111] *Id.* ¶ 135(a)(ii).
[112] *Id.* ¶ 131.

Importantly, while subscribers or providers of content, applications, or services may want to transmit as much traffic as they can without getting targeted for congestion management, they do not have an interest in causing congestion per se. If they know what congestion management practices are in effect, they may adjust their behavior – but that would not be "circumvention" so much as conforming their bandwidth usage to parameters established by the network provider. That would be beneficial to all involved.

Detailed disclosures about network operators' congestion management practices are necessary to facilitate this optimal result. Rather than casting the network as the battleground for an arms race between network operators implementing congestion management procedures and applications developers rushing to circumvent them, the Commission should encourage network operators to disclose all the details that applications developers would need to be mindful of how congestion is handled on the network while optimizing the performance of their products.

Security management presents exactly the opposite set of incentives. Network operators are seeking to minimize security threats on their networks while attackers are constantly seeking ways to ensure that their exploits succeed. Thus, highly detailed disclosures about exactly which spam emails, virus signatures, or malware profiles network operators are targeting would likely provide too much information to those with malicious intent while not reaping any substantial marginal benefit over a more generic disclosure.

Nonetheless, there is always the chance that legitimate network activity could be flagged as part of a network operator's security management procedures. It is therefore critical that the general contours and standards that operators use for making security management decisions be disclosed and that disclosure include information abut how users or applications providers can seek redress if they believe their traffic has been mistakenly flagged as a security threat.

The work of the Anti-Spyware Coalition (ASC)[113] provides a valuable example of how security management can be transparent without overexposing the details. The ASC is a group of anti-spyware vendors, consumer advocates, and academics dedicated to building consensus definitions and best practices in the debate surrounding spyware. Taken together, the ASC's seminal documents – the Definitions,[114] the Risk Model Description, [115] and the Best Practices[116] – provide common language and metrics that anti-spyware vendors can use to describe how they make decisions about which software to classify as spyware and why those decisions are made. All of these guidelines are written with sufficient detail such that software vendors can design their products to avoid being labeled as spyware, but not so detailed as to give malicious software authors a roadmap for avoiding detection.

The ASC has also published a Vendor Dispute Resolution Process[117] that sets out guidelines that anti-spyware companies can use to craft redress procedures for software vendors who

[113] CDT is the convener of the Anti-Spyware Coalition.
[114] Anti-Spyware Coalition, *Anti-Spyware Coalition Definitions Document* (Nov. 2007), http://antispywarecoalition.org/documents/2007definitions.htm.
[115] Anti-Spyware Coalition, *Anti-Spyware Coalition Risk Model Description* (Nov. 2007), http://antispywarecoalition.org/documents/2007riskmodel.htm.
[116] Anti-Spyware Coalition, *Best Practices: Guidelines to Consider in the Evaluation of Potentially Unwanted Technologies* (Mar. 2007), http://antispywarecoalition.org/documents/BestPracticesFinal.htm.
[117] Anti-Spyware Coalition, *Vendor Dispute and False Positive Resolution Process* (Nov. 2007), http://antispywarecoalition.org/documents/vendordispute.htm.

believe their products have been miscategorized as spyware. The Commission should encourage network operators to aim for the level of transparency for security management that the ASC has provided, perhaps with the aid of industry-standard terms and guidelines that build on and expand the work of the ASC and other consortia that have addressed other kinds of security threats.

3. More detail required if practices target specific applications or depart from standards

CDT believes that content- or application-specific congestion management practices should not be permitted under the rules. However, should some such practice be permissible, disclosure should include what content is targeted, how it is affected, what legitimate purpose is served, and direct notice to users whose traffic has been affected.

Likewise, CDT believes that any network management practices that depart from widely accepted standards should not generally be considered reasonable. If however, the Commission deems such a practice reasonable, it should be subject to more stringent disclosure requirements. The Internet is built on a series of open and accessible protocols, and any divergence from these standards could significantly limit the ability of innovators to reach Internet users. Consequently, any such deviation should be disclosed in detail for application developers who might have to adjust their innovations to ensure proper functioning in a non-standard environment.

4. Additional data to be disclosed

Aside from the details of network management practices, the proposed transparency rule would apply to "other practices" required for users and service providers to enjoy the protections of the present rules.[118] For subscribers to broadband Internet service to make the best use of their service, "other practices" must include certain basic elements describing the service. While CDT agrees that the proposed rules should remain lightweight and not overly prescriptive, here again the Commission should provide some guiding examples as to what information it considers "reasonably required" under the rule. As we have argued in the National Broadband Plan proceeding, this should include information concerning the connection's reliability, maximum and average expected speeds (throughput), latency within the broadband provider's network, and data concerning actual usage.[119]

In addition, broadband providers offering managed or specialized services should be required to report how the amount of broadband capacity they devote to such services compares to the amount of capacity they devote to Internet access. As the Commission has noted, exempting managed and specialized services from the present rules carries some risk that providers could fail to maintain and update the Internet portion of their networks in favor of those portions where they may exercise greater control.[120] Periodic disclosure of relative network capacities would provide an important check against this risk, allowing the Commission and interested members of the public to monitor, call attention, and respond to signs that an emphasis of managed or specialized services is causing open Internet access to be undersupported.

---

[118] NPRM app. A, Proposed Rules § 8.15.
[119] *Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future*, GN Docket No. 09-51, June 8, 2009, http://www.cdt.org/files/pdfs/20090608_broadband_comments.pdf.
[120] NPRM ¶ 153.

The Commission could, for example, require the reporting of this data in the form of averages of bandwidth provided in geographic areas where a broadband provider offers managed or specialized services over the same infrastructure as Internet access service. The important thing would be to ensure that data is reported in a consistent form that permits the tracking of trends over time and comparisons between broadband providers. The Commission should consider issuing a further notice of proposed rulemaking on how best to implement this kind of reporting.

C. Methods of disclosure

1. Public notice

With respect to the NPRM's questions as to how network management practices should best be disclosed, CDT agrees that the disclosure of general network management policies should be made publicly on providers' websites.[121] In light of the Internet's historic openness to all innovators, from large companies to small startups to individuals, it is critical that these disclosures be made publicly available to benefit not only subscribers, but also known and unknown content, application, and service providers.[122]

In addition to being minimally burdensome on providers (as compared to more targeted notice or prescriptive filing requirements), web-based notice affords a solution to the Commission's concern about balancing detail and usefulness to the average consumer.[123] The web easily facilitates a layered-notice approach, where an initial page contains a condensed disclosure that highlights the key points of the network operator's policy and links to a more complete disclosure page. Using this approach, providers can make granular details of network management practices available to sophisticated and interested users without bombarding average users with undesired information. There is some risk with this approach that top-level disclosures will be inadequate or even dissuade further exploration, but CDT believes Commission review of disclosures through the complaint adjudication process will be sufficient to address this concern.

2. Targeted notice to affected subscribers

As the Commission has suggested, disclosure provides important consumer benefits both before and after purchase.[124] Pre-purchase disclosure is important for comparing services, but it is not sufficient to address the concerns or questions of subscribers when they are or may soon be actually affected by congestion management practices. As noted above and in earlier CDT comments to the Commission, notifying individual subscribers about actual instances where

---

[121] *Id.* ¶ 126.

[122] Further, in light of paragraph 127's suggestion that *Computer III*'s comparably efficient interconnection (CEI) requirements might provide some guidance, we note that widely available public notice is consistent with the Commission's 1999 decision to require that Bell Operating Companies post their CEI plans publicly to benefit the then-increasingly competitive marketplace of Internet service providers. *See Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services*, 14 FCC Rcd 4289, 4297-4302 (1999), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1999/fcc99036.txt.

[123] NPRM ¶ 126.

[124] *Id.* ¶ 125.

network management practices come into play can help them make efficient use of broadband service and for troubleshoot perceived connection problems.[125]

In addition to pre-purchase disclosure of management practices, therefore, broadband providers should be encouraged to provide targeted notice when a subscriber's Internet traffic is, may soon be, or has been affected. This could take the form an automated notice sent to the subscriber or an account management page or "dashboard" provided for the subscriber to monitor usage of the service.[126] While advance or real-time notification would be ideal – for example, a system that alerts users when they are approaching usage caps or when their usage triggers congestion management practice – the Commission need not create prescriptive requirements or get into the operational details. What is important for present purposes is that the final rule recognize the importance of targeted notice in addition to general public disclosure.

3. Disclosure to government

With regard to disclosure to the Commission, CDT believes that the FCC should craft a streamlined reporting system that allows it to receive the text of the publicly posted information (and changes to it) while minimizing any regulatory burden on broadband providers. Broadband providers should not be required to explain or justify changes to their posted information at the time of submission, but instead simply required to inform the Commission of what changes were made. To minimize regulatory burden, the FCC should not require extensive additional information, with one exception.

The exception is that the providers should be required to disclose how the network capacity they have dedicated to Internet access services compares to the capacity dedicated to unregulated managed or specialized services. While not as likely to be of use to average consumers and thus not necessary for inclusion in public disclosures of network management practices, this information will be a useful resource for the Commission as well as watchdog groups or journalists interested in ensuring continued investment in infrastructure dedicated to the open Internet. CDT therefore proposes that this information be regularly reported to the Commission, as discussed in paragraph B.4 above.

D. Privacy issues

CDT agrees with the Commission's view, expressed in paragraph 130, that disclosure of network management practices will not likely implicate personal information. To the extent, though, that broadband providers offer tools enabling subscribers to track their own usage data or provide targeted notice to subscribers when their traffic has been affected by network management practices, the broadband providers should not be permitted to use the information for marketing or similar purposes, and should take steps to secure such information against

---

[125] *Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, Feb. 13, 2008, at 7-8, http://www.cdt.org/speech/20080213_FCC_comments.pdf; *Reply Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket No. 07-52, Feb. 28, 2008, at 8-9, http://www.cdt.org/speech/20080228_FCC_comments.pdf.

[126] As one example, Comcast recently began testing a usage dashboard for its Internet subscribers. *See, e.g.*, Todd Spangler, *Comcast Tests Data-Usage Meter in Oregon: Feature Lets Subscribers See How Much Internet Bandwidth They Use*, MULTICHANNEL NEWS, Dec. 1, 2009, http://www.multichannel.com/article/391268-Comcast_Tests_Data_Usage_Meter_In_Oregon.php.

disclosure to third parties. Data that is collected and retained for the purpose of putting it in the hands of subscribers should be used and disclosed for that purpose only.

VII. Reasonable Network Management

CDT agrees with the Commission's proposed approach of leaving the precise contours of "reasonable network management" to case-by-case adjudication,[127] but the Commission can and should provide some high-level guiding principles concerning what kinds of practices are likely to be considered "reasonable" and what kinds are not. In addition, CDT believes the NPRM's conception of network management is unnecessarily broad; actions empowering individual subscribers to control or personalize their experience and actions aimed at social policy goals should not be conflated with managing the network so that it operates effectively and safely. With respect to the role of standards bodies, the Commission should express its expectation that reasonable network management tactics will comply with standard technical protocols, while recognizing that standards bodies are not in a position to render case-by-case policy judgments about whether particular network management practices are or are not "reasonable."

A. Limiting principles

The NPRM offers an open-ended definition of "reasonable network management;" the definition includes "reasonable" actions taken for one of several enumerated purposes (mitigating congestion, addressing unwanted traffic, preventing unlawful conduct) as well as "other reasonable network management practices."[128]

Under this definition, the paramount question is what qualifies as "reasonable." It should be clear, and the Commission should clearly state, that a network management practice is not necessarily "reasonable" simply because its purpose is among those enumerated in the definition. For example, specific practices intended to mitigate congestion may be unreasonable despite their valid purpose. This was the case with the practices at issue in the Comcast Order, which were intended to address congestion but were rejected by the Commission because of the means they used to do so.[129]

CDT agrees that the Commission should leave the "precise contours" of what will qualify as "reasonable" to be fleshed out in future adjudications.[130] In its current form, however, the NPRM fails to provide even principle-level guidance. Rather than leave industry participants, innovators, and future regulators to extrapolate based on a few examples, the Commission should set forth some high-level principles for analyzing reasonableness. These principles need not be codified in the actual rules, but the Commission should make clear that network management practices that run afoul of these principles will not be deemed reasonable. Alternatively, the Commission could say that falling short on these principles will create a strong presumption of unreasonableness, rebuttable only by a clear showing that the practice offers benefits for at least some Internet traffic; that the practice does not carry risks of material

[127] NPRM ¶ 134.
[128] *Id.* ¶ 135.
[129] *See* Comcast Opinion and Order, 23 FCC Rcd 13028, ¶ 51 (2008) ("Comcast's conduct poses a substantial threat to both the open character and efficient operation of the Internet, and is not reasonable.").
[130] NPRM ¶ 134.

adverse effects for other Internet traffic; and that there is no readily available better alternative.[131]

First, the FCC should say that reasonableness determinations will focus on the goal of preserving the Internet's open nature. Specifically, a network management practice should not be considered reasonable if its widespread adoption would carry a risk that providers of independent content, services, or applications could, as a practical matter, come to find that their ability successfully to reach and serve the subscribers of a particular broadband provider depends on obtaining some kind of permission, approval, or favorable classification from that broadband provider.

For purposes of this principle, what matters is the *effect* a practice could have if implemented widely. The possibility that the *intent* of the practice may be benign should not be relevant. Nor should the possibility that the practice, in its initial form, may be of such small scale (e.g., applying only to a small amount of traffic) as to have little concrete impact on the overall Internet environment. Practices that over time could create gradually rising entry barriers for independent speakers and innovators should not be deemed "reasonable."

Second, the FCC should say that network management, to be considered reasonable, should be based on general criteria that are applied evenly. In other words, it should not enable a provider of broadband Internet access service to play favorites by singling out specific content, applications, or services for special or inferior treatment on an ad hoc basis.[132] This principle may apply differently in the context of congestion mitigation than in the context of combating harmful or unwanted traffic, as discussed under each respective section below. But the core point is that invoking network management arbitrarily, such that the provider of broadband Internet access services is in a position to pick and choose which specific content, applications and services to favor and which not, forces innovators to start worrying whether and how their offerings might be targeted. Relying instead on generally applicable criteria minimizes this risk.

Third, the FCC should express the strong expectation that reasonable network management tactics will comply with the common technical standards on which the Internet is based. The Internet has been described as a "network of networks," and common protocols with generally accepted technical standards (such as the TCP/IP suite of protocols) are what enable communications and applications to traverse its constituent networks on a seamless basis. Developers of applications rely on and design technology with the expectation that applications built to use and respond to these standards will function the same way across the public Internet. Network management tactics that depart from key standards risk increasing instability across the Internet, causing applications and services to behave in unexpected ways and complicating the task facing innovators.

Finally, as discussed in Part VI above, reasonable network management practices should be expected to be sufficiently transparent to consumers and to providers of Internet content, applications, and services. With respect to consumers, disclosures should be sufficient to avoid

---

[131] *See, e.g.*, Canada Radio-Television and Telecommunications Commission, *Review of the Internet Traffic Management Practices of Internet Service Providers*, Telecom Regulatory Policy, CRTC 2009-657 (Oct. 21, 2009), http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm (articulating a similar approach).

[132] CDT does not mean to imply that different providers of broadband Internet access service must employ the *same* criteria. Different providers may well use different criteria for determining when and how to engage in network management.

surprise and misunderstanding on the part of a broadband provider's subscribers. With respect to providers of online content, applications, and services, transparency should be in sufficient detail to enable them to understand when and how their online offerings may be affected.

B. Managing congestion and service quality

For network management aimed at mitigating congestion, a broadband provider should rely on objective criteria, such that all content, applications, or services with similar bandwidth usage patterns receive similar treatment. There is simply no reason, if the aim is to address congestion issues, to treat two applications differently if the quantity and patterns of their bandwidth usage are comparable. Congestion management practices should be agnostic as to both the content of subscribers' communications and the identities of the parties with whom the subscribers are communicating.

As the NPRM suggests, however, it is perfectly reasonable for congestion management tactics to focus on the volume of bandwidth demands that different subscribers are making on the network. Thus, temporarily limiting the bandwidth available to subscribers using "a substantially disproportionate amount of bandwidth" would be reasonable; so would the imposing usage limits or usage-sensitive pricing on subscribers.[133] All of these tactics rely on metrics that are objective and quantifiable: volume or patterns of bandwidth usage. What matters is *how much* traffic a subscriber sends and receives, not what that traffic is.[134]

The NPRM also asks about practices that would seek to address service quality by prioritizing classes of latency-sensitive over classes of latency-insensitive traffic.[135] As a preliminary matter, CDT believes that the use of the term "quality-of-service" in the proposed definition of "reasonable network management" is inappropriate, for the reasons discussed above.[136] The definition should instead refer to "service quality." On a more substantive level, CDT has concerns that this kind of traffic management system would require providers of broadband Internet access service to monitor how their subscribers are using their Internet connections and would raise questions about how each broadband provider classifies different applications, especially newly emerging ones.[137] As discussed above, CDT believes service quality issues would be much better addressed via practices allowing *subscribers* to designate which of their traffic streams should be prioritized.[138]

C. Managing harmful or unwanted traffic

Practices aimed at addressing harmful or unwanted traffic should also be based on some general criteria that the provider of broadband Internet access applies evenly to all traffic. The

---

[133] NPRM ¶ 137. Indeed, CDT has long argued that some form of usage-sensitive pricing, perhaps targeting only the highest volume users, may be the most straightforward way of controlling excessive bandwidth usage in an evenhanded manner. *See, e.g.*, *Reply Comments of the Center for Democracy & Technology In the Matter of Broadband Industry Practices*, WC Docket 07-52, Feb. 28, 2008, at 7, http://www.cdt.org/speech/20080228_FCC_comments.pdf.

[134] As discussed above, the timing of a subscriber's bandwidth usage may also be relevant. *See supra* Part V.B.1. Timing, like volume, provides an objective criterion that can be applied evenly regardless of a communication's content, application, or service.

[135] NPRM ¶137.

[136] *See supra* Part II.C.

[137] CDT's concerns with traffic-class prioritization are set forth more fully above. *See supra* V.D.

[138] *See supra* Part V.B.2.

criteria will need to be different, however, from those used for practices addressing congestion. Bandwidth usage will not be the relevant metric, for example. Indeed, focusing on the content or source of a communication might be essential; communications might be blocked precisely because they contain a virus or originate from a known spammer.

To be considered reasonable, however, this type of network management practice should still be based on criteria that can be applied to all traffic in an evenhanded manner. A broadband provider should have criteria for identifying and responding to harmful and unwanted traffic. Such criteria may need to be qualitative in many cases, rather than the more quantitative criteria should govern congestion management. But the work of the Anti-Spyware Coalition (ASC) provides an example that shows it is possible to establish relatively objective criteria to identify harmful malware.[139] In addition, reasonable network management practices in this area should create some process for considering the claims of parties who feel their traffic has been wrongly classified as harmful or unwanted. The Anti-Spyware Coalition has endorsed a redress process for considering claims that software has been wrongly tagged as spyware.[140]

The general outlines of a provider's policy on harmful and unwanted traffic – though not the detailed algorithms it may use to identify such traffic – should be publicly available.[141] Policies and criteria would need to be sufficiently general and amendable to leave network operators with ample leeway to identify and respond quickly to the evolving nature of security threats, malware, spam, and other harmful or unwanted traffic. But policies would also ensure that network management practices in this area are not merely ad hoc or arbitrary.

CDT disagrees, however, with the NPRM's suggestion that actions to block particular traffic (e.g., pornography) to individual subscribers who have requested such blocking should be considered "network management."[142] While "network management" is not a term of art with a fixed and widely accepted definition, CDT believes that the term has most commonly been understood to refer to technical actions that network operators take, at the network level, to keep the network running efficiently, to avoid network-related problems, and to minimize security threats to the users. The term is best reserved for efforts to centrally manage the *network* on behalf of the general body of subscribers. By contrast, carrying out the express choices of individual subscribers amounts to providing personalization features, add-on services, or user empowerment tools on a subscriber-by-subscriber basis. The thing being "managed" is the experience of the individual user, and the user is making the choice of how to manage it.

CDT strongly supports the provision of such optional "user empowerment" features and tools, but does not believe they should be classified as network management. Treating them as network management is entirely unnecessary, because they do not run any risk of violating the Commission's rules in the first place. The proposed rules bar interference with content, applications, and services *of the user's choice*.[143] User empowerment tools do not interfere with user choice; indeed, they promote it. Nor should it constitute "discrimination" for a provider of broadband Internet access service to block traffic based the wishes of the subscriber. Treating

---

[139] *See* Anti-Spyware Coalition, *Anti-Spyware Coalition Risk Model Description* (Nov. 2007), http://antispywarecoalition.org/documents/2007riskmodel.htm.
[140] Anti-Spyware Coalition, *Vendor Dispute and False Positive Resolution Process* (Nov. 2007), http://www.antispywarecoalition.org/documents/vendordispute.htm.
[141] *Supra* Part VI.
[142] NPRM ¶ 138.
[143] *See id.* App. A, Proposed Rules §§ 8.5, 8.7.

actions like individualized, user-activated pornography blocking as "network management" serves no real purpose, other than to stretch the term to the point where its meaning is almost entirely elastic.

D. Preventing unlawful conduct

The Commission should delete items (a)(iii) and (a)(iv) from the definition of "reasonable network management" – the portions of the definition that refer to the prevention of unlawful conduct.

CDT agrees that unlawful communications do not deserve protection under the Commission's open Internet rules. But classifying actions to prevent unlawful conduct as "reasonable network management" is entirely unnecessary to achieve the Commission's goal of "emphasiz[ing] that open Internet principles apply only to lawful transfers of content."[144] The relevant proposed rules (sections 8.5, 8.7, 8.9 and 8.13) are each expressly limited to protecting *lawful* communications. Unlawful Internet communications are simply outside the scope of the rules. There is no reason, therefore, to include this topic within the "reasonable network management" exception. Where the rules by their very terms don't apply in the first place, no exception is necessary.

Lumping actions to prevent unlawful conduct into the category of network management improperly conflates very different concepts raising very different policy questions. Actions to prevent unlawful conduct do not protect the network or subscribers of the network; rather, they serve social policy goals. Those goals may be important; child pornography and copyright infringement, to use the two examples cited in the NPRM, are indeed serious problems. But such social policy goals have nothing to do with ensuring "robust, safe, and secure Internet access to [] subscribers,"[145] as the NPRM reasonably characterizes the core focus of network management. Network management is about making the network run well and safely, not about furthering various social policies.

Moreover, stretching the definition of "reasonable network management" to include actions to prevent unlawful conduct could be interpreted to imply that the Commission endorses or encourages actions by providers of broadband Internet access service to actively scour their networks for unlawful material. Given the difficult policy questions such actions raise, the Commission should not go down this dangerous path.

The policy questions center on the inevitably fact that actions targeting unlawful Internet communications will have at least some impact on perfectly lawful communications as well. First, to identify the unlawful communications, a provider of broadband Internet access would likely have to start engaging in the wholesale inspection of its subscribers' transmissions – many if not most of which will be entirely legal. Scrutinizing subscriber communications on a widespread basis raises serious privacy issues. Internet users simply do not expect their broadband Internet access providers to be regularly examining the content of their Internet communications. It is likely that some subscribers will not use the Internet as extensively as they otherwise would if they believe their access provider is watching, just as they would be wary of the telephone if they believed all phone conversations were being wiretapped.

[144] *Id.* ¶ 139.
[145] *Id.* ¶ 140.

In addition, determining when individual communications are unlawful may be easier said than done. Efforts by providers of broadband Internet access service to identify unlawful conduct might be countered by wider use of encryption – leading to an arms race between broadband providers and customers and ultimately slowing down network performance due to increased computer processing demands. Reliably identifying copyright infringement is greatly complicated by the difficulty of distinguishing "fair use" of copyrighted material from infringing use. The tricky, case-by-case legal judgments this requires cannot likely be performed by automated technologies and could leave providers of broadband Internet access – or, for that matter, the Commission – dealing with uncomfortable legal questions outside their areas of expertise.

The Commission should not venture unnecessarily into these issues. Indeed, doing so would be at odds with Commission's goals in this proceeding. The point of this proceeding is to *preserve* a network architecture that has proved highly successful. A core attribute of that architecture is the lack of gatekeeper control at the network level. Moreover, Congress has on several occasions indicated that Internet access providers should not be held broadly responsible for controlling the behavior of Internet users.[146] Encouraging providers of broadband Internet access service to take on a new function as police, judge, and jury with respect to the legality of Internet communications would be a radical recasting of the role of access providers. This proceeding should focus on preserving the successful elements of the existing Internet model, not restructuring it.

E. The "catch-all" provision

Item (b) in the definition of "reasonable network management" is characterized by the NPRM as a "catch-all."[147] CDT does not object to the inclusion of language providing flexibility for currently unanticipated future steps that might be warranted, as the NPRM says, "to maintain the proper functioning of [the] networks" and "provide robust, safe, and secure Internet access to subscribers."[148]

The language of (b), however – "other reasonable network management practices" – is entirely unbounded. It also renders the definition tautological: "reasonable network management" consists of reasonable network management practices. CDT therefore would recommend modifying (b) to read:

(b) other reasonable practices that a provider of broadband Internet access service may take with respect to its network to protect and promote the smooth, effective, and safe operation and enjoyment of that network.

F. The role of standards bodies

Having spent more than a decade participating in technical standards bodies such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), CDT firmly believes in the power that open standards can have in supporting the most efficient and interoperable experience for all Internet users regardless of the network, platform, or location

[146] *See* 47 U.S.C. § 230 (stating that an Internet service provider shall not be treated as a speaker or publisher of content supplied by any third party); 17 U.S.C. § 512(a) (limiting Internet service provider liability for transmitting infringing material by a third party).
[147] NPRM ¶ 140.
[148] *Id.*

from which they access the Internet. It is thanks to standardized protocols that disparate computer networks can interoperate, enabling communications and applications to traverse the Internet on a seamless basis – without standards, the Internet could not exist. The use of standardized protocols also provides crucial assurances for applications developers that their applications will function in a similar way all across the Internet.

The Commission has asked for comment on the role that standards bodies such as the IETF can play in helping to define what network management practices are reasonable.[149] In CDT's view, the key standards-related criteria for evaluating a network management practice is whether the practice complies with existing standards. Network management practices that run counter to widely accepted standards risk increasing instability on the network, complicate the task of innovators aiming to develop new applications for the Internet, and can even "break" existing applications and services.

Furthermore, given the wealth of standardized congestion management protocols at their disposal, network operators have few excuses for departing from standards. Standardizing mechanisms to mitigate network congestion has been a central focus of the IETF since its earliest days. The most foundational of these mechanisms is the Transmission Control Protocol (TCP), which provides a way for end hosts to alter their transmission rates when they sense congestion on the network.[150] For decades, TCP has served as the Internet's most important and widely adopted congestion control mechanism.

In the years since TCP was created, the IETF has sought to optimize and extend TCP's performance in multiple ways. Explicit Congestion Notification (ECN) allows the network to be more proactive in signaling congestion to end hosts.[151] Active Queue Management techniques, such as Random Early Detection (RED), help to reduce some of the detrimental side effects that result when routers' packet queues become full.[152] Newer efforts currently underway include Multipath TCP,[153] which would allow two end hosts to find the least congested route between them among multiple paths, and Congestion Exposure,[154] which would give network nodes greater insight into potential upcoming network congestion. Encouraging standards compliance would likely aid in the uptake of each of these mechanisms.

The IETF has also been extremely responsive to network operators' recent concerns over increased congestion caused by peer-to-peer (P2P) traffic. Soon after the Comcast-BitTorrent issues came to light, the IETF (with CDT's input) organized a workshop focusing on P2P-related congestion,[155] which in turn led to the formation of two new working groups in 2008: Low Extra Delay Background Transport (LEDBAT)[156] and Application-Layer Traffic Optimization (ALTO).[157]

---

[149] *Id.* ¶ 141.
[150] Information Sciences Institute, University of Southern California, *Transmission Control Protocol*, IETF RFC 793 (Jon Postel ed., Sept. 1981), http://www.ietf.org/rfc/rfc793.txt.
[151] K. Ramakrishnan & Sally Floyd, *A Proposal to Add Explicit Congestion Notification (ECN) to IP*, IETF RFC 2481 (Jan. 1999), http://www.ietf.org/rfc/rfc2481.txt.
[152] Bob Braden et al., *Recommendations on Queue Management and Congestion Avoidance in the Internet*, IETF RFC 2309 (Apr. 1998), http://www.ietf.org/rfc/rfc2309.txt.
[153] IETF, *Multipath TCP (mptcp)* (Oct. 2009), http://www.ietf.org/dyn/wg/charter/mptcp-charter.html.
[154] IETF, *Congestion Exposure BoF (ConEx)* (Oct. 2009), http://trac.tools.ietf.org/area/tsv/trac/wiki/re-ECN.
[155] Jon Peterson & Alissa Cooper, *Report from the IETF Workshop on Peer-to-Peer (P2P) Infrastructure, May 28, 2008*, IETF RFC 5594 (July 2009), http://www.ietf.org/rfc/rfc5594.txt.
[156] IETF, *Low Extra Delay Background Transport (ledbat)* (Aug. 2009), http://www.ietf.org/dyn/wg/charter/ledbat-charter.html.

LEDBAT is standardizing a congestion control mechanism that peer-to-peer applications can use to yield to more latency-sensitive applications (like VoIP) in times of congestion. ALTO is developing a protocol that would allow peer-to-peer applications to learn valuable information about network characteristics and topology that those applications can then use to decide with whom to peer. By including standards compliance as one criterion in evaluating network management practices, the FCC will be supporting these and future promising standards efforts that specifically address congestion caused by peer-to-peer traffic, while also providing extra incentives for network operators to participate in standardization efforts.

Mere standards compliance does not guarantee that a particular network management practice is reasonable, however. For example, a network operator could use the IETF-standardized Differentiated Services (DiffServ) architecture, which allows traffic to be classified into different service levels, to single out and de-prioritize the traffic of one particular application that competes with a service offered by the operator, all in the name of network management. This should be considered an unreasonable practice under most circumstances, despite it being standards-compliant.

Because reasonableness determinations go beyond the question of compliance, it is unrealistic to expect standards bodies to pass judgment or to assist the FCC in passing judgment on the reasonableness of individual operators' practices. At its core, the IETF is an engineering organization dedicated to crafting technical protocols that improve the Internet. While the standards it creates most certainly have policy implications, the IETF's expertise lies not in making policy judgments about what constitutes a reasonable practice, but in providing tools to help network operators manage their networks in the most efficient and interoperable fashion. In some rare cases, the IETF has expressed its disapproval of non-standard practices,[158] but such cases are the exception.

Furthermore, the IETF has gone to significant lengths to stay out of adjudicating disputes between individual companies, including the kinds of disagreements that may arise between network operators and applications providers when operators' congestion management practices unreasonably discriminate against a particular application or class of applications. Individuals participate in the IETF, not companies; company affiliations may be known, but an individual's IETF contributions are never ascribed to his or her employer. Commissioner McDowell has suggested that the optimal approach for the FCC would be to merely "spotlight instances of market failure" and refer them to collaborative bodies like the IETF, but the IETF deals explicitly with generic, Internet-wide problems, not disagreements between individual companies in the marketplace.[159] Those disagreements are precisely where FCC action, guided by a set of limiting principles, is needed.

The opportunity that the this rulemaking provides, therefore, is not to recruit standards bodies into the business of evaluating how particular network operators make use of standardized protocols, but to promote the widespread use of the standards themselves. This distinction is especially compelling in the context of copyright protection, where the Commission has sought

---

[157] IETF, *Application-Layer Traffic Optimization (alto)* (Nov. 2009), http://www.ietf.org/dyn/wg/charter/alto-charter.html.
[158] *See, e.g.*, Internet Architecture Board, *IAB Commentary: Architectural Concerns on the Use of DNS Wildcards* (Sept. 2003), http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html; Sally Floyd, *Inappropriate TCP Resets Considered Harmful*, IETF RFC 3360 (Aug. 2002), http://www.apps.ietf.org/rfc/rfc3360.html.
[159] NPRM, Statement of Commissioner Robert M. McDowell Concurring in Part, Dissenting in Part.

comment on how standards bodies may help determine the legality of the transmission of particular content.[160] No standards body that CDT is aware of – and certainly not the IETF – has the tools or the mandate to automatically distinguish a lawful transmission from an unlawful one. Certain technologies, such as digital fingerprinting and watermarking, have been developed to automate the process of identifying content. However, even the providers of these technologies and their industry standards organizations are incapable of judging whether a particular transmission is lawful or not, since the mere existence of particular content on the network does not necessarily imply legality or illegality in each context (a particular transmission may be licensed or considered fair use, or it may be legal in one jurisdiction but not another, for example). As noted above in paragraph D, we do not believe the FCC should delve into these issues in this proceeding, but in any event standards bodies would be unlikely to be of help.

Commissioner McDowell has also suggested that collaborative standards bodies have "never failed to resolve major network management challenges."[161] This claim may be easily disputed – the continued proliferation of spam is an obvious counterexample. More importantly, however, the claim seriously overstates the role of standards organizations. The goal of standards bodies like the IETF is to create interoperable solutions to network problems. Standards bodies cannot require network operators to comply. The litany of standards, such as the IPv6 standard, that are widely considered to be useful or even necessary but remain largely undeployed or underdeployed attests to that fact. Nor are standards bodies in a position to sanction individual companies acting unreasonably, whether those companies are standards-compliant or not. For these reasons, the FCC should encourage standards compliance, but it cannot rely solely on standards bodies to ensure that network management practices continue to support Internet openness and nondiscrimination.

VIII. Defining Managed or Specialized Services

Providers of broadband Internet access service may also develop and deploy other services that are not themselves Internet services, but that, in whole or in part, use the same broadband equipment and facilities as the providers' Internet access offerings. Indeed, this is common today: cable providers deliver cable television and broadband Internet access services over the same physical plant, for example. The proposed rules state that any non-Internet access service will not be covered by the open Internet rules.[162]

There are major risks, however, in the NPRM's use of the term "managed or specialized services" without providing any definition. Because the term is undefined, it easily could be misinterpreted to include activities that in fact are occurring over the Internet, that are the functional equivalent of Internet access, or that have serious negative impacts on the providers' Internet access offerings. The term could, in other words, create gaping loopholes in the Commission's rules.

CDT believes that there are benefits in allowing broadband providers to offer *non-Internet access* services that are not subject to the open Internet rules. However, such services must be supplements or additional offerings to a provider's Internet access service, not replacements for

[160] *Id.* ¶ 141.
[161] *Id.*, Statement of Commissioner Robert M. McDowell Concurring in Part, Dissenting in Part.
[162] *See id.* App. A, Proposed Rules § 8.1 ("These rules apply to broadband Internet access service providers only to the extent they are providing broadband Internet access services.").

it, and must not significantly harm such offerings. To reduce the risk of creating a loophole that would undermine the effectiveness of the open Internet regime, the rules need to cabin the concept of "managed or specialized services" by defining the term, and the Commission needs to demand certain disclosures and make clear that it will take action where it finds the managed or specialized services exception to be undermining the intent of the rule. CDT's suggested approach and specific recommendations for rule modifications are set forth in section C. below.

A. Potential benefits of exempting managed or specialized services from the rules

Traditionally, "managed services" have been business-class offerings providing, for example, "virtual private networks" and dedicated connections between corporate offices and business partners. CDT certainly agrees that such non-consumer-focused offerings should not be prohibited by neutrality rules. Beyond such offerings, managed or specialized services may allow providers to experiment with service offerings that might not be feasible to deliver over the regular Internet for technical or business model reasons. The classification provides an avenue for further experimentation by network operators and for meeting needs that the ordinary Internet proves unable to fulfill.

CDT is highly skeptical that there are consumer-oriented content, applications, or services that are suited to carriage on the Internet but that would suffer significantly impaired availability or quality if forced to operate under the open Internet rules. The traditional Internet, openness and all, has proved so far to be suitable for a wide range of innovations by clever engineers and programmers. Nonetheless, if there were to be some potential offerings that simply could not be delivered effectively to users who want them under the regime set forth in the rules, then the possibility of delivering them as distinct managed or specialized services would provide a path forward. Properly defined, the category of managed or specialized services can provide a key response to any claims, rhetorical or otherwise, that open Internet rules will make the effective delivery of certain services impossible.

It is hard to predict precisely what functions might be delivered via managed or specialized services. As a matter of terminology, CDT would recommend using "managed services" to refer to transmission offerings aimed at enterprise users and "specialized services" to refer to services that involve transmissions to individual consumers. Thus, managed services would likely include private transmission services providing guaranteed or highly secure connectivity between the branch offices of a large business. The category might also include the provision of highly reliable telemedicine transmissions between medical facilities, as might be required for any kind of remote participation in or control of real-time medical procedures.[163]

[163] Telemedicine applications have sometimes been cited as an example of a valuable service that could be stifled by a nondiscrimination rule. *See, e.g.*, Robert E. Litan, *Catching the Web in a Net of Neutrality*, WASHINGTONPOST.COM, May 2, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/01/AR2006050101061.html. Most medical applications, however, involve simple exchanges of data that is not highly sensitive to latency. CDT is highly skeptical that it would make sense to use the public Internet, even with some form of prioritization, to carry transmissions of medical data that are so critical that any delay or disruption would jeopardize someone's health. Because Internet traffic traverses multiple carriers' networks, individual carriers cannot guarantee end-to-end service quality. In the last mile, communications lines are at risk of downed trees and wires, cut cables, and other common problems that can knock out consumer offerings. Any telemedicine application that requires 100% reliability would need to be carried on dedicated and redundant facilities. In other words, it would be offered as a managed or specialized service, and would be very unlikely to be carried on a residential-grade shared Internet access network.

Specialized services, meanwhile, would include the provision of high-speed data links giving consumers a special communications connection with particular entities or for particular functions. For example, a provider of broadband Internet access could team with a particular movie studio to create a "specialized service" offering consumers a speedy link for downloading or streaming the studio's latest HD movies. Or the provider could work with a hospital to provide fully reliable two-way communications between a patient's home medical devices and the hospital facilities where those devices will be remotely monitored and calibrated. Or the provider could offer special transmission capability to support HD videoconferencing for interested subscribers.

Depending on the business model, a provider of a specialized service might look to the subscriber for payment, might charge a content or service provider with whom it is partnering (in the examples above, the movie studio, hospital, etc.), or some combination. But regardless of who ultimately foots the bill, there is no question that for any of the examples cited above, the *broadband provider* exercises substantial control over the services' functions. The broadband provider selects particular content partners or decides what particular, specialized capabilities to offer. The broadband provider probably initiates the service itself, or at least affirmatively decides whether, when, and how to proceed. With respect to this category of services, in other words, the broadband provider has centralized, gatekeeper control. Managed and specialized services do not share the open characteristics of the Internet.

B. Potential risks of exempting managed or specialized services from the rules

It is perfectly reasonable for services that are not Internet access to deliver only those capabilities selected or approved by the broadband provider. Not every service needs to follow the open model of the Internet. But if managed or specialized services were to begin to replace, squeeze out, or marginalize the Internet's open model, the goals of this proceeding would be placed in serious jeopardy. There are at least two ways that managed or specialized services could crowd out Internet services.

First, the Commission could allow such a loose definition of "managed or specialized services" that broadband providers are effectively able to reclassify selected Internet traffic as "managed or specialized service" traffic – and therefore exempt that traffic from the open Internet rules. In this scenario, the "managed or specialized service" is not really a distinct transmission service, but rather a means of boosting the priority of certain Internet traffic. The broadband provider sells priority treatment to a content provider; labels this transaction as the sale of a "managed or specialized service" for regulatory purposes; and then delivers that content provider's content to subscribers via the same bandwidth as all other Internet traffic, but with special router-level priority.

This would be indistinguishable from the paid priority that the NPRM's proposed nondiscrimination rule is intended to prevent. If broadband providers are free to carry Internet traffic and "managed or specialized" traffic intermingled on the same bandwidth, while prioritizing the "managed or specialized" traffic, then the nondiscrimination rule will be effectively moot; all it would take to sidestep the rule would be to characterize the prioritized traffic as "managed or specialized."

Second, even if broadband operators keep their Internet access services and their managed or specialized services distinct, they could act in ways that steer subscribers to use and rely on the

managed or specialized services instead of Internet access. In particular, a network operator could devote the bulk of its maintenance and capacity upgrade resources to specialized services, while allowing the Internet access services to lag. It could build up its specialized services to provide substitute offerings for the main online functions Internet users expect today – but at state-of-the-art speeds.

The risk here is of gradual erosion. Over time, the provider's Internet access services could lose ground to managed or specialized services that enjoy more bandwidth. More and more activity could shift to managed or specialized services, as content providers and end users alike find the performance of ordinary Internet traffic to be inferior. The open Internet rules would apply to a dwindling portion of the network, and the Internet's openness would be of diminishing benefit to independent innovators due to its small capacity. The NPRM alludes to this risk in paragraph 153, when it asks, "[w]ill network providers provide sufficient capacity for robust broadband Internet access service on shared networks used for managed or specialized services?"

C. Recommendations

To minimize the first risk described above, the Commission should provide a definition of "managed or specialized services" that limits its ability to serve as a loophole. To minimize the second risk, the Commission should call for periodic disclosure of bandwidth information to expose problems as they start to develop.

CDT recommends adding the following definition to the Commission's proposed rules:

Managed or specialized broadband transmission service. Any communication service by wire or radio that:
(a) provides broadband data transmission:
(i) between an end user and a limited group of parties or endpoints; or
(ii) for a limited set of purposes or applications;
(b) is not intended, marketed, or widely used as a substitute for broadband Internet access service, either individually or together with other managed or specialized services offered by the same provider; and
(c) either:
(i) does not traverse the public Internet at all; or
(ii) is allocated bandwidth on last-mile transmission facilities that is separate from bandwidth allocated to broadband Internet access service, such that usage spikes for the managed or specialized service do not affect the amount of last-mile bandwidth available for broadband Internet access service.

In addition, the definition of "broadband Internet access" should be changed to include a reference to managed or specialized services:

Broadband Internet access. Internet Protocol data transmission between and end user and the Internet. Broadband Internet access shall not include:
(a) dial-up access requiring and end user to initiate a call across the public switched telephone network to establish a connection; or
(b) any managed or specialized broadband transmission service.

The first definition above would ensure that "managed or specialized services" are not merely Internet access services by another name (minus the openness). Clause (a) requires that the service actually be specialized, rather providing a general-purpose platform akin to Internet access service. Clause (b) safeguards against the possibility of a service that, while limited in the sense that it does not permit connection to the entire Internet, nonetheless allows such a wide range of communications or functions that it might be perceived or marketed as a viable alternative to Internet access. For example, a service might be called "Web Select" and provide access to the "best" 500 Web sites and online services, as selected by the network operator – including at least a choice or two for all of today's common online functions, from Web mail to auction sites to social networking to online music and video. Such a service, which aims to mimic the functions of Internet access, should not be exempt from the open Internet rules.

Nor should the rules exempt the offering by a provider of a *group* of managed or specialized services that, bundled together, offer such functionality. For this reason, the last portion of (b) in our proposed definition expressly refers to groups of services.

Clause (c) would ensure that the "managed or specialized services" category is not just a label that can be applied to whatever portion of Internet traffic a broadband access provider wishes to favor or prioritize. To be treated as a managed or specialized transmission service, the transmission actually needs to be special. It may use the same physical facilities as ordinary Internet traffic, but it must have a separate allocation of bandwidth.

Meanwhile, the modified definition of "broadband Internet excess" – expressly excluding managed or specialized services from the definition – would ensure that services that qualify as "managed or specialized services" will not be covered by the open Internet rules.

This would not, however, imply that all managed or specialized services automatically are exempt from Commission regulation entirely. As defined above, the category of "managed or specialized services" is broad enough to include non-Internet broadband transmission services such as cable services regulated under Title VI. In CDT's view, "managed or specialized services" may include not only "services that have not been classified by the Commission,"[164] but also services that fall within other regulatory classifications. Treatment as a "managed or specialized service" should simply mean that the open Internet rules do not apply.

Finally, even with an appropriately cabined definition, there remains the possibility that broadband providers could devote most new capacity to their managed and specialized services and fail to provide robust capacity for Internet access service. The Commission should make clear that it will be watching carefully for any signs of this kind of gradual erosion of the open Internet and will not tolerate it. If the Commission requires that providers of broadband Internet access periodically report how much bandwidth they allocate to broadband Internet access and how much to managed or specialized services, any disparities should be readily apparent before the problems become severe. Broadband Internet access providers that are failing to invest in bandwidth for Internet access service could not only be subject to criticism and pressure from the Commission, watchdog groups, Internet users, and ultimately the marketplace, but also could be at risk of action from the Commission.

[164] NPRM ¶ 148.

In particular, the Commission could find that the provider's "managed or specialized services" are now serving as substitutes for Internet access. Under clause (b) of CDT's proposed definition, this could cause them to lose their "managed or specialized services" status and subject them to the openness rules. Given the potential for such reclassification, this is an area where transparency could well prevent problems from developing in the first place.

As discussed above, therefore, the Commission should require that broadband providers, when providing broadband Internet access service and managed or specialized broadband transmission services in the same geographic markets, disclose how much bandwidth they allocate to each category of service.[165] In addition, the Commission should expressly state that it will look at this question every year in its report on broadband deployment pursuant to section 706 of the Telecommunications Act of 1996. Specifically, the annual 706 Report should expressly address what impact, if any, the offering of managed or specialized broadband transmission services appear to be having on the robustness of broadband Internet access service.

IX. Application of the Internet Principles to Wireless

CDT agrees that the proposed rules (with the above modifications) should apply to all broadband Internet access service delivery platforms, including wireless. As network capacity and device capability grow, people are increasingly using mobile Internet access in much the same ways as wireline access. 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.[166] Broadband use and the benefits it provides would suffer if the move toward mobile access were to come at the expense of Internet openness.

Given the technical realities of wireless networks, however, what constitutes reasonable network management on a wireless data network might differ from that of wired connections. As the NPRM notes, wireless networks are subject to conditions such as access point sharing, interference, and more constrained bandwidth[167] – that might require more aggressive traffic management to ensure the smooth and effective operation of the network. The Commission should state that it will take account of such considerations in analyzing and determining the reasonableness of network management practices in the wireless context.

At the same time, CDT does not anticipate that the Commission would need to disregard the key principle, discussed above, that network management should not single out specific content, applications, or services for special treatment. In general, wireless network management aimed at dealing with capacity and congestion challenges should still be based on evenhanded factors such as usage volume – that is, the demands that individual subscribers place on the network – and not on the content of particular subscribers' communications. To use the NPRM's example,

---

[165] *See supra* Part VI.B.4.

[166] *See Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future*, GN Docket No. 09-51, June 8, 2009, at 12, http://www.cdt.org/files/pdfs/20090608_broadband_comments.pdf; *Reply Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future*, GN Docket No. 09-51, July 21, 2009 at 8, http://www.cdt.org/files/pdfs/20090721_fcc_broadband_comments_3.pdf.

[167] NPRM ¶¶ 159, 172.

wireless carriers should be free to set stricter volume caps or limits on bandwidth, but not to block video applications outright.[168] What should be relevant to the broadband provider is the amount of bandwidth being used, not the content and services that are flowing over that bandwidth.

One other consideration for wireless networks is the treatment of non-Internet traffic, particularly mobile voice telephone calls. The Commission has noted that the proposed rules will not apply to voice traffic,[169] and has asked for comment on the effect the proposed rules will have on this service.[170] The largest wireless broadband networks grew out of wireless telephone networks, and many users still view voice telephony as the core and most important function of their mobile communications service. Based on this history, it should not be considered unreasonable for a wireless provider to give its voice traffic priority. Even if delivered over the same bandwidth as Internet traffic, voice service is an application for which many consumers have special expectations. To the extent that prioritizing specific applications is generally impermissible under the final non-discrimination rule, the Commission should give specific notice that prioritization of legacy voice services will be considered reasonable network management for wireless networks.

* * *

This proceeding presents an opportunity to ensure that the dynamic growth and innovation seen on the Internet over the past 15 years can continue. CDT looks forward to working with the Commission to refine its proposed rules.

Respectfully submitted,

Leslie Harris
David Sohn
John Morris
Alissa Cooper
Andrew McDiarmid
Jonathan Dunn

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

January 14, 2010

[168] *Id.* ¶ 173.
[169] *Id.* ¶ 156.
[170] *Id.* ¶ 171.