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

In the Matter of	)	
	)	
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 notices, numbered DA 08-91 and DA 08-92, seeking comment in the above-captioned proceeding. CDT is a non-profit, public interest organization dedicated to preserving and promoting free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet.

Introduction and Summary

CDT strongly believes that 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." Actions by broadband providers to degrade certain Internet traffic – the central subject of the petitions on which the Commission has sought comment – may in some instances have legitimate motives but also pose risks of increased gatekeeper control. A full policy response to such risks, however, likely requires congressional action. In these comments, CDT argues that:

1. The Commission should not assert jurisdiction to adopt formal rules regulating the network management practices of broadband Internet access providers;

2. The Commission should clearly establish that degrading the performance of a user's chosen service, application, or device is inconsistent with the Commission's broadband Policy Statement;

3. Where a carrier degrades traffic for network management purposes, its policies should be reasonably transparent, evenly applied, and consistent with core internetworking standards; and

4. The Commission should consider how it might play a useful monitoring and fact-finding role.

1. The Commission should not assert jurisdiction to adopt formal rules regulating the network management practices of broadband Internet access providers.

As discussed below, CDT believes that broadband provider actions that degrade the performance of lawful Internet applications or content can pose serious concerns for the innovative and open nature of the Internet. The risks are real, and any Commission response to the pending petitions should be careful not to suggest otherwise. Indeed, there is a strong argument for establishing a policy framework to safeguard certain core characteristics of the Internet that have proven central to its remarkable success.[1]

At the same time, the Commission should be wary of proposals that would involve asserting jurisdiction to regulate the way broadband providers handle and manage broadband Internet traffic. In CDT's view, the task of establishing a concrete policy framework with carefully targeted rules for broadband network operator behavior is one for Congress. If legislation on the topic is enacted, the Commission might well have a key enforcement role. But in the absence of such legislation, CDT believes it would not be appropriate for the Commission on its own authority to devise and implement a regulatory regime mandating or prohibiting specific behaviors.

[1] *See* Center for Democracy & Technology, *Preserving the Essential Internet* (June 2006) (available at http://www.cdt.org/speech/20060620neutrality.pdf).

Restraint is warranted to avoid setting the dangerous precedent that the Commission has general regulatory authority over the broadband Internet. Even rules that are well intentioned and well devised could effectively set such a precedent, potentially opening the door to less judicious regulatory intervention in the future. The Commission should recognize that the public interest is best served by taking a cautious approach to the agency's possible jurisdiction over broadband Internet matters, not by asserting what would amount to unguided discretion to regulate broadband how and when the agency sees fit.

Therefore, CDT does not believe that the Commission should initiate a rulemaking proceeding on the question of what does and does not qualify as "reasonable network management." The adoption of formal rules dictating what network management practices are permitted would likely exceed the Commission's current legal authority, and in any event would constitute an overbroad assertion of Commission regulatory authority from a policy perspective.

2. The Commission should clearly establish that degrading the performance of a user's chosen service, application, or device is inconsistent with the Commission's broadband Policy Statement.

Completely blocking users' ability to access certain Internet content, services, or applications is clearly inconsistent with the Commission's broadband Policy Statement.[2] But as CDT catalogued in its June 15, 2007, comments in this docket, outright blocking of Internet traffic is just one of a number of possible network operator practices that involve some form of differential treatment for different traffic. Some forms of

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

differential treatment seem unobjectionable, while others would present real risks for openness and innovation on the Internet.[3]

Affirmatively degrading selected traffic is an example of a practice that is likely to be harmful in most instances.[4] When traffic is selected for degradation based on its content or the identity or type of the associated service or application, the risks to competition and innovation are serious. Particular competitors or innovators could be placed at a significant competitive disadvantage. More broadly, innovators looking to launch new applications might find that network operator approval and cooperation has become a precondition for good transmission quality. This would undermine a key factor behind the Internet's unique openness – the ability of innovators to reach Internet users everywhere without having to coordinate or strike deals with the users' Internet access providers.

The application of the Policy Statement to practices that degrade the performance of certain applications is unclear. On their face, the principles set forth in the Statement say that users are entitled to access the Internet content of their choice, but say nothing about the quality, speed, or reliability of such access. CDT agrees with Free Press and

---

[3] Comments of the Center for Democracy & Technology, WC Docket No. 07-52 (June 15, 2007) (available at http://www.cdt.org/speech/20060615fcc-neutrality.pdf) ("CDT Comments"). The Appendix at the end of those comments included a table listing a full range of possible "discriminatory" practices without expressing any policy judgment about them; CDT offered its evaluation of different practices on pages 7-12.

[4] Degrading traffic involves detaining, dropping, or otherwise impairing the delivery of some packets even when there is sufficient available bandwidth to transmit them onward – with the result that the affected traffic streams get less than "best efforts" delivery. Professor Edward Felten has used the term "non-minimal discrimination" to describe the same type of practice. *See* Edward W. Felten, *Nuts and Bolts of Network Neutrality*, Princeton University (Jul. 6, 2006) at 3. This can be distinguished from prioritization, in which delivery of lower priority packets is slowed only when the network is congested and only for as long as it takes to enable the higher priority packets to go first.

others, however, that the Policy Statement would mean next to nothing if degrading applications were considered entirely outside its scope.[5] After all, degrading traffic can serve largely the same ends as blocking, if it impairs the performance of a particular service or application to the point that users desert it (or never give a new service a sufficient chance in the first place). Like outright blocking, degradation can permit the network operator's decisions, rather than the preferences of users, to determine what online services and applications will succeed.

CDT therefore suggests that the Commission move to clarify that degrading particular applications or classes of applications is inconsistent with the Policy Statement (subject, as discussed below, to the same "reasonable network management" exception that applies to the Policy Statement generally). It could do this by issuing a declaratory ruling, as advocated in the petition filed by Free Press and others. Alternatively or in addition, it could add a new principle to the Policy Statement. In its prior comments, CDT urged the Commission to adopt a new nondiscrimination principle along the following lines:

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,* consumers are entitled to access and use the content, applications, services, and devices of their choice without unreasonable discrimination by their network provider with respect to speed, service quality or price.[6]

CDT continues to support this kind of nondiscrimination principle. If the Commission would prefer that a new principle focus more narrowly on degradation, another possible formulation could read:

---

[5] Free Press et al., Petition for Declaratory Ruling, CC Docket Nos. 02-33, 01-337, 95-20, 98-10, GN Docket No. 00-185, CS Docket No. 02-52, WC Docket No. 07-52 (filed Nov. 1, 2007) ("Free Press et al. Petition") at 17.
[6] CDT Comments at 14.

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,* consumers are entitled to access and use the content, applications, services, and devices of their choice without intentional degradation by their network provider of the performance of the particular content, applications, services, or devices.

CDT believes that clarifying the Policy Statement's applicability to intentional degradation is important to ensuring the usefulness of the Policy Statement in the ongoing policy debate. The principles set forth in the Statement already lack the status of formal rules. If in addition the Statement focuses narrowly on blocking and turns a blind eye to crucial questions of degradation and discrimination – central issues for the Internet's continued openness – it will be rightly perceived as being of negligible help in preserving "the vibrant and open character of the Internet."[7]

3. Where a carrier degrades traffic for network management purposes, its policies should be reasonably transparent, evenly applied, and consistent with core internetworking standards.

The Commission's Policy Statement notes that its provisions "are subject to reasonable network management."[8] Thus, clarifying that the provisions of the Policy Statement cover degradation would still leave open the possibility that individual instances of degradation could qualify as reasonable network management practices. For example, degradation, no less than outright blocking, presumably would be a reasonable traffic management practice when used to control spam or denial-of-service attacks.

As discussed above, the Commission should not issue rules regulating precisely what constitutes permissible network management in the broadband Internet context. CDT believes, however, that there are several key principles that should guide both

[7] Policy Statement ¶5.
[8] Policy Statement n.15.

network operators and policymakers as they consider questions relating to network management.

First, network management practices involving degradation (or, for that matter, prioritization) of selected traffic should be disclosed publicly. Disclosure need not go into technical detail sufficient to provide a roadmap for evading traffic management policies relating to spam and other network attacks. But there is no legitimate reason why a network operator cannot clearly disclose the basic contours and impact of its policy. In the case of a policy involving degradation, the carrier should explain what legitimate security or network management purpose is served, what the criteria are for selecting the traffic to be degraded, and the basic method of degradation. If specific content, applications, or services are targeted, that would be particularly important to disclose.

Transparency can provide an important safeguard, enabling consumers and consumer advocates to push back against practices that could negatively affect competition or impair the usability of particular applications. It also can enable consumers to compare – to the extent they have a competitive choice – different broadband providers to see which one has traffic management policies that best meet the consumer's individual needs. A heavy BitTorrent user, for example, might be very interested to know which of the broadband providers in his local area degrades high bandwidth traffic as a means of controlling congestion. Transparency also can encourage developers of services and applications to shape their products' bandwidth usage patterns in ways that take account of legitimate network congestion considerations.

But consumers cannot exert marketplace pressure against practices they do not know are occurring. In the absence of disclosure, the average broadband subscriber has no way to determine if or when traffic is being degraded by her network operator. When a certain online site or service performs poorly, many consumers will likely assume that the problem lies with the provider of the site or service. Poor performance could be due to the provider having insufficient server capacity to meet demand, insufficient Internet connectivity, or poor quality software. But if in fact the subscriber's own Internet provider has caused the slowdown or other problem, subscribers should have an accessible and effective means of finding that out.

There may be a role for government to press for disclosure of traffic management policies involving degradation. CDT is not certain, however, whether the Commission is best positioned or even has jurisdiction to address this issue. The Federal Trade Commission would be another possible candidate, but ultimately it may be up to Congress to determine where to assign responsibility.

A second principle is that network management practices involving degradation should be evenly applied. Policies that single out specific content, applications, or services for degraded treatment are magnets for mixed motives and possible abuse. So are policies that single out specific classes of services or applications. Such policies give the network operator – rather than competitors, innovators, and users – control over which types of applications and services will work best from a technical perspective. This can leave the network operator with a great deal of power to constrain innovation and competition, based on how the network operator chooses to classify new protocols or applications that do not fit an established category.

A much better approach would be to tie degradation to a generally applicable bandwidth-related policy. For example, a traffic management policy stating that no application may consume more than 20 percent of overall available bandwidth on shared network facilities at any time could result in delays for some packets of bandwidth-intensive applications, but it would not unfairly skew competition so long as the policy is evenly applied and suitably disclosed. It should be possible to develop network management practices that apply evenly based on criteria that are both objective and relevant to the network management purpose.[9] Quantity and patterns of bandwidth usage may be relevant to network management purposes; the specific content or function of a particular packet stream is not.

A third principle is compliance with core internetworking standards. The Internet has often been described as a "network of networks." It is largely thanks to common protocols with generally accepted technical standards (such as the TCP/IP suite of protocols) that disparate computer networks can interoperate, enabling communications and applications to traverse the Internet on a seamless basis. Developers of applications rely and design technology based on these standards, with the expectation that applications built to utilize and respond to standard internetworking protocols will function the same way across the public Internet.

---

[9] As an alternative to network management practices that involve restricting or degrading high bandwidth usage, network operators could institute pricing policies that make heavy bandwidth users pay more. Time Warner recently announced a trial of usage-based pricing. *See, e.g.,* Kenneth Corbin, *Time Warner to Test Usage-Based Broadband Pricing*, InternetNews.com (Jan. 17, 2008) (available at http://www.internetnews.com/infra/article.php/3722516). In CDT's view, charging for high-volume usage could discourage excessive bandwidth consumption and spur applications developers to make their products more bandwidth-efficient, while at the same time putting all online services on an equal footing and steering clear of technical interference with user traffic.

Network management practices that run counter to key industry standards risk increasing instability across the Internet, and in CDT's view should be avoided. Given the vast proliferation of Internet-based applications, a network operator considering a departure from generally accepted standards cannot possibly have a firm grasp on what particular applications may fail or behave in unintended ways as a result of the change. Moreover, departures from standards complicate the task of innovators aiming to develop new applications for the Internet.

A current example of a practice in tension with key standards is Comcast's reported injection of TCP RST ("reset") packets to terminate certain peer-to-peer file-sharing connections and thereby reduce congestion on the network. The use of TCP resets for congestion control has been expressly discouraged by the Internet Engineering Task Force (IETF), the Internet's longest-established technical standardization body. In describing best practices for the use of TCP resets, an IETF standards document "recommend[s] that the TCP reset not be used as a congestion control mechanism," because this clouds the true meaning of the TCP reset packet as it is expressed in the TCP protocol specification, and may cause applications that use TCP to change the way they react to TCP resets in general.[10]

In other words, applications would no longer be able to assume that receipt of a TCP reset packet during a communication between two computers reliably means that the sending computer has "hung up" and terminated the connection. Applications built on the assumption that a TCP reset packet has that particular meaning might be impaired. Just as important, applications might start responding to TCP resets not by waiting and

[10] S. Floyd, Inappropriate TCP Resets Considered Harmful, RFC 3360 (Aug. 2002) (available at http://www.ietf.org/rfc/rfc3360.txt?number=3360) at 3.

trying to reestablish a connection later, but rather by aggressively trying to resend immediately, since the true cause of the reset packet would now be ambiguous.[11] This could be true not just on the specific network electing to use TCP resets for fighting congestion, but on all the networks where the applications operate.

In short, CDT believes that departing from generally accepted standards can carry significant and widespread costs. Network operators should look for other ways to handle network management issues.

4. The FCC should consider how it might play a useful monitoring and fact-finding role.

As discussed above, in the absence of legislation establishing an overall policy framework, the Commission should not attempt to impose a regulatory regime governing the network management practices of broadband providers. The Commission may, however, be able to play a useful monitoring and fact-finding role.

The Commission's 2007 Notice of Inquiry, aimed at identifying actual network management practices, was a sensible step in this regard.[12] As CDT observed in its comments, however, there may be limits to the information such a proceeding can elicit.[13] Among other reasons, examples of network management practices with arguably harmful effects or motives are unlikely to be voluntarily self-reported, and third parties will rarely be in a position to document carriers' internal practices.

Future efforts to gather information could include direct and specific queries to network operators. In addition, the Commission could consider conducting a survey or

---

[11] *See id*. at 3 (warning of the risk of "aggressive behavior from TCP implementations in response to a reset").
[12] *Broadband Industry Practices*, Notice of Inquiry, FCC 07-31 (rel. Apr. 16, 2007).
[13] CDT Comments at 4-7.

study of the capabilities being built into modern broadband networks. For example, to what extent is new network equipment offering new functions for inspecting, classifying, degrading, or prioritizing network traffic? The capabilities being offered and the investments being made to deploy them may offer at least as much insight into future traffic management plans – and perhaps into potential risks they may entail -- as any currently observable behavior.

* * *

CDT appreciates the opportunity to comment on these important questions.

Respectfully submitted,

Leslie Harris
David Sohn
John Morris
Alissa Cooper
Center for Democracy & Technology
1634 I Street, N.W. Suite 1100
Washington, DC 20006
(202) 637-9800

February 13, 2008