

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

In the Matter of)	
)	
Broadband Industry Practices)	WC Docket No. 07-52
)	
)	

**REPLY COMMENTS OF THE CENTER FOR DEMOCRACY &
TECHNOLOGY**

The Center for Democracy & Technology (“CDT”) respectfully submits these reply 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. CDT submitted initial comments on February 13, 2008.

CDT does not believe the Commission should try to adopt rules regulating network management practices. In these reply comments, however, CDT emphasizes that:

- The Commission should take this opportunity to provide some principle-level guidance relating to discrimination, by amending its broadband Policy Statement;
- Network management policies aimed at security threats are different from those aimed at congestion, and the two may warrant separate policy analyses;
- Network providers managing traffic for congestion reasons should seek evenhanded means, such as usage-based pricing; and
- Increased transparency concerning traffic management practices is both feasible and necessary.

1. Arguments emphasizing that network management is necessary and beneficial provide no reason for the Commission to refrain from providing principle-level guidance through its broadband Policy Statement.

Many commenters stress that network management is needed to address real problems.¹ Spam, viruses, denial-of-service attacks, and other threats to network security often require strong, network-level responses. In addition, network management may play an important role in responding to the challenges of rising overall traffic volume and the tendency of certain users and/or applications to consume a high proportion of available bandwidth.

The real policy question here, however, is not whether network management in general is necessary; it is whether there are specific forms of network management that may pose significant concerns. As many commenters note, “network management” is a broad term that can encompass many different techniques and practices.²

CDT does not believe the Commission should embark on a course of detailed regulation of these various network management techniques through formal rules. As CDT argued in its initial comments, devising and implementing a regulatory regime mandating or prohibiting specific behaviors would constitute an overbroad assertion of Commission regulatory authority over the broadband Internet.³

At the same time, the Commission need not and should not send the message that any and all actions taken in the name of network management are entirely benign. The Commission should take this opportunity to provide some guidance and establish some

¹ See, e.g., Comments of The United States Telecom Association (“USTA Comments”) at 10-12; Comments of Comcast Corporation (“Comcast Comments”) at 11-19; Comments of AT&T, Inc. (“AT&T Comments”) at 6-11.

² See, e.g., Comments of Verizon and Verizon Wireless (“Verizon Comments”) at 19-20.

³ Comments of the Center for Democracy & Technology (“CDT Comments”) at 2-3.

baseline expectations by adding a non-discrimination or non-degradation principle to its broadband Policy Statement.

Adopting a principle along the lines suggested in CDT's initial comments⁴ would indicate the Commission's recognition that network provider discrimination or degradation that targets specific content or applications poses significant policy risks. To be sure, there will be times when discrimination is justified, as discussed below, by reasonable traffic management goals. But there should be a baseline expectation that broadband providers will not exercise unlimited discretion to discriminate against selected traffic, just as the Commission's current Policy Statement establishes a baseline expectation that broadband providers will not exercise unlimited discretion to block selected traffic.

In short, just because network management in general may be a necessary and beneficial activity, it does not follow that the activity should be free of principles and scrutiny to help shape – without dictating the details through prescriptive rules – the forms that network management will take.

2. Comments suggest that, in considering network management practices, it may be important to separate tactics aimed at protecting users from spam or malware from tactics aimed at controlling bandwidth usage by legitimate users.

Some comments imply that regulatory intervention limiting network management could impair efforts to fight spam, spyware, viruses, denial-of-service attacks, and other

⁴ CDT Comments at 5-6.

security threats.⁵ Protecting subscribers against such threats is a very different goal from addressing particularly high bandwidth usage by legitimate individual subscribers.⁶

Where the focus of network management is security-related, the aim is to shield subscribers from communications that they almost certainly do not want, and indeed that may be affirmatively intended to cause harm. Certain incoming traffic may be blocked or degraded, but it is traffic with a purpose widely viewed as illegitimate, if not outright malicious or illegal. Absent an error, therefore, there should be no negative impact whatsoever on any subscriber's intended use of the network.

Significantly, for this type of traffic management, discrimination based on the content or source of a communication may be essential. The broadband provider targets certain traffic precisely because the content includes a virus or advertises a phishing scam, or because the source is a known spammer.⁷

Protecting subscribers from the indirect, congestion-related effects of heavy bandwidth usage by other subscribers presents a very different scenario. In this case, there will be some negative impact (though perhaps of small magnitude in some cases) on certain subscribers' intended uses of the network. And because the real issue here is volume of usage – not protecting users from harmful incoming traffic – there is no inherent need for the traffic management practices to focus on the content or source of the communication. (It might be necessary to keep track of which traffic is associated

⁵ See, e.g., AT&T comments at 24-25.

⁶ See Verizon Comments at 3, 18-20 (noting that there are “myriad” purposes for network management, and describing security and congestion as two of the different possible goals).

⁷ See Verizon Comments at 24 (“For example, broadband providers seek to trace identified threats to particular port numbers, or even sometimes to specific IP addresses, that appear to be the source of the threat, and then filter traffic coming from that location.”).

with certain high-volume subscribers, but the parties those subscribers choose to communicate with or the specific applications they use are not inherently relevant.)

In light of these differences, the key principles of objectivity and transparency – as highlighted by CDT in its initial comments and discussed further below – may apply differently to the two cases. Network providers need considerable leeway to identify security threats, malware, and spam, and to respond quickly. So long as providers disclose their security and consumer protection traffic management policies and criteria at a general level, and then offer some reasonable process for considering the claims of parties who feel they have been wrongly classified as threats, there should be little risk.

For network management practices aimed at bandwidth conservation and congestion control, however, objective criteria and a higher degree of transparency are both feasible and necessary.

3. Network management practices targeting congestion should be evenly applied.

While network capacity presumably will expand over time, there will always be some bandwidth constraints. Network management techniques may offer important tools for addressing those constraints. But techniques that put a network provider in the position to pick and choose among applications, services, or protocols – deciding which ones will be allowed to use how much bandwidth or which ones will be subject to limits – carry considerable risks. Network management practices of this kind have the potential to turn the network provider into a gatekeeper, able to determine which new applications or protocols will thrive and which will not.

This risk is present even where the congestion-related goal is completely legitimate. Once a network operator is in the business of selecting particular traffic for

inferior treatment, there is the possibility of mixed motives, as choices between different tactics for addressing congestion problems could be tinged by competitive considerations. Innovators, meanwhile, would need to start worrying about whether and how the network operator might choose to target their applications.

As CDT suggested in its opening comments, these risks can be mitigated if network management policies are based on objective criteria and applied evenly, so that all applications with similar bandwidth usage patterns receive similar treatment.⁸ Comcast, perhaps recognizing this general principle, makes a point of characterizing its traffic management techniques as “based on purely objective criteria.”⁹

The analogy to congestion-linked stop lights on highway entrance ramps, which several commenters offer in explaining the role of traffic management policies,¹⁰ may help illustrate this point. The stop lights allow a certain number of vehicles to merge onto the highway at a certain pace. Their operation may depend on congestion conditions or the time of day, but when they are operating they apply to all vehicles equally. They do not, for example, treat vehicles differently depending on the type of vehicle, the identity of the driver, or the driver’s destination or reason for using the highway. In contrast, if the local traffic or highway authority reserved full discretion to pick and

⁸ CDT Comments at 8-9. Alternatively, as CDT stated in comments submitted in this docket on June 15, 2007, any policy that allows each subscriber to select specific applications or content for special traffic handling seems perfectly benign. So long as the choice lies with the subscriber, there is no risk of the network provider playing favorites. *See* Comments of the Center for Democracy & Technology, WC Docket 07-52 (Jun. 15, 2007) (available at <http://www.cdt.org/speech/20060615fcc-neutrality.pdf>) at 8.

⁹ Comcast Comments at 4; *see also id.* at 27 (stating that Comcast’s tactics are “based on objective criteria applied equally to all Internet protocols.”); *id.* at 36-37 (“[T]o determine whether any protocol should be managed, Comcast uses purely objective criteria . . . [T]his is entirely content- and identity-neutral and certainly not discriminatory.”).

¹⁰ USTA Comments at 11; Comcast Comments at 29.

choose which drivers would be subject to red lights and for how long, without any clear and public criteria, it could exercise significant influence over businesses and individuals who need to use the highway.

Perhaps the most straightforward way of controlling excessive bandwidth usage in an evenhanded manner would be to impose surcharges on the heaviest users. This would discourage excessive bandwidth use and lead consumers and applications developers to avoid wasteful or inefficient application design. Some commenters suggest that usage-based pricing would be unpopular with consumers,¹¹ but the vast majority of users would not be affected at all if usage fees target only the highest volume users.¹² CDT agrees with those commenters who argue that usage-based pricing may offer a better way of addressing the problem of individual “bandwidth hogs” than ad hoc actions by network providers to limit or target specific applications.¹³

By contrast, charging a flat rate regardless of usage volume gives users no economic reason to control or economize on volume, and thus no reason to press applications developers for more bandwidth-efficient applications. It should be no surprise, given this pricing model, that some users are choosing to employ bandwidth-

¹¹ See Comments of Frontier Communications (“Frontier Comments”) at n.6.

¹² The great bulk of broadband subscribers use amounts of bandwidth that pose no concerns for network providers, even under current flat-rate contracts; only a tiny percentage are what providers may consider excessive users of bandwidth. See Comcast Comments Attachment B, *Frequently Asked Questions about Excessive Use* at 1 (stating that “a very small number [of Comcast High-Speed Internet customers] – well less than 1% – use excessive amounts of bandwidth . . . beyond what is permitted under the AUP”); see also Comments of Time Warner Cable Inc. at 11 (“consumption patterns have resulted in fewer than five percent of users consuming as much as 60-70 percent of all available bandwidth”).

¹³ See Comments of Vonage Holdings Corp. at 4-5; Comments of the Information Technology and Innovation Foundation at 9-10. In addition, some large broadband providers cite a move towards more usage-based pricing as a possibility. See AT&T Comments at 22; Verizon Comments at 38.

hungry applications including peer-to-peer technology. Such applications do not “shift costs . . . to ISPs without the ISPs’ consent,” as some commenters would have it.¹⁴

Rather, the consumers who choose to use such applications are merely taking full advantage of the terms the network provider has offered them. They were offered a flat rate plan with no clear bandwidth usage limits, and they are choosing to use applications that behave accordingly. If that dynamic is unsustainable, network providers should take a careful look at their pricing model, not point fingers and single out particular applications for degraded treatment.

4. Greater transparency is needed in order for marketplace forces to provide a meaningful safeguard.

Some commenters argue that competition in the marketplace provides an ample safeguard against network management practices that would harm consumers or innovation.¹⁵

As many commenters also observe, however, competition requires transparency. Network providers cannot compete on the relative merits or demerits of their traffic management practices if consumers have no reasonable way of determining what those practices are. And as Comcast points out, consumers who encounter technical problems in using various online applications and services often are confused about what the real cause of the problem is. It may well be, as Comcast says, that many problems subscribers attribute to network management practices in fact are “completely unrelated

¹⁴ Comments of Laurence Brett Glass at 4; *see also* Frontier Comments at 3. If ISPs’ Terms of Service included specific, quantitative bandwidth usage limitations, then perhaps one could argue that users exceeding those limitations are shifting costs to their ISPs without consent. The major U.S. broadband ISPs, however, do not generally include specific bandwidth usage limitations in their Terms of Service.

¹⁵ *See, e.g.*, USTA Comments at 7, 15; Comments of CTIA – The Wireless Association at 3-5.

to the Internet service they purchase from their broadband service provider.”¹⁶ This helps to highlight, however, that there is no easy way for consumers to determine when and whether network management is a factor in any degraded performance they experience.

Disclosure of network management practices is therefore essential. Moreover, disclosures need to do more than simply allude vaguely to the fact that the carrier engages in “certain network management practices” and cite the generic purpose (presumably, ensuring acceptable performance for all subscribers). To be useful, disclosures must be specific enough to provide some basis for comparison between providers. CDT believes that broadband providers should provide an informative description of their traffic management policies, including the nature of the criteria used to trigger management actions and to target specific traffic or applications.¹⁷

Some commenters argue that detailed transparency concerning network management is impractical, on grounds that it would be too burdensome for network providers, would merely confuse subscribers, or would undermine the effectiveness of the management techniques.¹⁸ But it should be possible to provide disclosure at a level that steers clear of these concerns.

First, a meaningful description of a provider’s general network management tactics and policies need not include updates every time the provider tweaks a spam filter or otherwise adjusts specific thresholds or algorithms in

¹⁶ Comcast Comments at 30.

¹⁷ Comcast’s comments in this proceeding go further than most disclosures of traffic management practices have to date, explaining that the company targets P2P unidirectional upload sessions when congestion in a neighborhood reaches a predetermined level. Comcast Comments at 27.

¹⁸ See AT&T Comments at 33; Verizon Comments at 16; Comcast Comments at 41.

response to real-time congestion concerns. Disclosing all tweaks could well be burdensome, but it should not be necessary.

Second, descriptions of network management practices need not be featured prominently on (for example) each customer's bill. Perhaps descriptions of network management practices could confuse some non-technical consumers if aggressively called to their attention. But a description in the Terms of Service and on a network provider's public website would enable those subscribers who care about such things to investigate, without confusing others. It also would enable product reviewers to analyze and compare different policies and share that information with a general audience.

Third, disclosure need not go into substantial detail about tactics aimed at fighting malware, spam, and security threats. As discussed above, this type of network management should have no negative impact on any subscriber's chosen use of the network, so more limited transparency should not raise major fairness concerns. (Network providers should, however, have some means of addressing claims that their security policies have mistakenly impaired innocent traffic.) Transparency concerning security-focused traffic management also carries the greatest risk of facilitating evasion, since the parties responsible for harmful traffic are unscrupulous and probably highly motivated to evade the network provider's filters or limits.

For network management aimed at congestion control, however, more descriptive disclosures are warranted. Again, it would not be necessary to include all the technical details. But better disclosure of the criteria used to target traffic

for management, rather than facilitating hacking and evasion, could well prompt applications developers to try to avoid the targeted behavior. If applications adjust their bandwidth usage patterns to reflect the provider's traffic management policies, that should promote the network provider's purpose, not hinder it.¹⁹

* * *

As explained in its initial comments, CDT does not believe the Commission should assert jurisdiction to impose a regulatory regime governing the network management practices of broadband operators. Certain general principles, however – including transparency, evenhandedness, and compliance with core internetworking standards – should guide network operators and policymakers as they consider network management questions. The Commission should consider non-regulatory means, such as modifications to its broadband Policy Statement and continued monitoring and fact-finding, for promoting such principles.

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 28, 2008

¹⁹ Verizon notes that some applications, include Slingbox and some multi-player online games, dynamically adjust bandwidth usage based on current bandwidth availability in the network. Verizon Comments at 31. Far from being a problem, this kind of intelligent approach to bandwidth usage is something network providers should try to encourage and shape, by adopting transparent traffic management policies that will become part of the bandwidth availability landscape to which the applications respond.