Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	
Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators	WC Docket No. 07-52
Petition for Declaratory Ruling Regarding Internet Management Practices	
Broadband Industry Practices	

REPLY COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

Fred von Lohmann
Peter Eckersley
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

February 28, 2008

REPLY COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

The Electronic Frontier Foundation (EFF) submits these reply comments in response to the comments filed by Comcast Corporation (Comcast)[1] and others in response to the Public Notices issued by the Wireline Competition Bureau on January 13, 2008.[2] In particular, these reply comments respond to the question of whether Comcast's intentional interference with certain peer-to-peer (P2P) traffic violates the Commission's *Internet Policy Statement*.[3]

EFF was among the first to independently test and discover the precise nature and scope of Comcast's P2P interference efforts.[4] Based on that research, as well as Comcast's actions both before and after disclosure of the research results, EFF concludes that Comcast has run afoul of the *Internet Policy Statement* in one crucial respect: it has persistently failed to adequately disclose to customers and competitors the nature and scope of its P2P interference activities.

EFF accordingly urges the Commission to clarify that "reasonable network management," as that term is used in the *Internet Policy Statement*, necessarily incorporates (at a minimum) a strong norm of transparency, and that Comcast's behavior has fallen short of that norm.[5] Such a clarification will send a strong message to Comcast and other ISPs regarding the minimum conditions necessary if market forces are to play their part in disciplining ISPs and serving the interests of consumers.

I. INTRODUCTION.

EFF agrees with the many commenters who have stressed the necessity of network management by ISPs in general. EFF also believes that, when it comes to separating "good" network management from "bad," market forces should be preferred, whenever possible, to regulation. Acknowledging these truisms, however, is merely the beginning, rather than the end, of the inquiry.

In order for market mechanisms to serve their proper role in policing the network management practices of ISPs, transparency is critically important. Participants in the market (whether they be competitors, customers, or innovators) must have adequate information regarding those network management practices. For example, if an ISP fails to adequately disclose the nature of its "network management" activities with respect to particular P2P protocols (even after being repeatedly asked by consumer groups and its own customers, as Comcast was here[6]), market mechanisms may be disrupted

[1] Comments of Comcast Corp., WC Docket No. 07-52, filed Feb. 12, 2008 (hereafter, "Comcast Comments").

[2] Public Notice, Wireline Competition Bureau, FCC, *Comments Sought on Petition for Declaratory Ruling Regarding Internet Management Policies*, DA 08-91, WC Docket No. 07-52 (Jan. 14, 2008); Public Notice, Wireline Competition Bureau, FCC, *Comments Sought on Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators*, DA 08-92, WC Docket No. 07-52 (Jan. 14, 2008).

[3] In re Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities, Policy Statement, 20 FCC Rcd. 14986 (2005) (hereafter "*Internet Policy Statement*").

[4] *See* EFF White Paper, *Packet Forgery By ISPs: A Report on the Comcast Affair*, November 2007 (<http://www.eff.org/wp/packet-forgery-isps-report-comcast-affair>, appended hereto as Attachment A) (hereafter "EFF Comcast White Paper").

[5] EFF today simply urges the Commission to clarify its existing *Internet Policy Statement*, using Comcast's activities as an illuminating example of conduct that fails to meet the norm of transparency implicit in the concept of "reasonable network management." EFF expresses no view on whether the *Internet Policy Statement* is independently enforceable, or whether the Commission possess statutory authority to engage in rulemaking in this area.

[6] *See* Section VI below.

in several ways:

- Customers will not be able to express their preferences by "voting with their wallets" (*i.e.*, switching ISPs). The customer may instead blame the application vendor, or believe the protocol is inferior, or assume that any dissatisfaction is the result of his own technical missteps.
- Competing ISPs will have difficulty marketing alternative broadband plans that include superior approaches to network management to customers who might prefer them. This would retard the normal market incentives that would otherwise encourage competing ISPs to assiduously upgrade their broadband networks.
- Innovators will be left guessing about the technical "baseline" of what constitutes "Internet access," making it difficult for them to develop new applications and protocols that work reliably without asking the prior permission of ISPs. In this fashion, the withholding of information about network management practices can operate as a *de facto* barrier to entry for new Internet technology developers.

Of course, market mechanisms may not be a panacea for every situation where an ISP might flout the principles set forth in the *Internet Policy Statement* under the guise of "reasonable network management." But market mechanisms provide a first line of defense against anti-competitive or anti-consumer behavior by ISPs. And without adequate transparency regarding the nature and scope of network management activities by ISPs, those mechanisms will be stymied.

II. THE PRINCIPLE OF TRANSPARENCY IS IMPLICIT IN THE NOTION OF "REASONABLE NETWORK MANAGEMENT."

A. Transparency Regarding Network Management Serves the Interests of Consumers.

The Commission stated in its *Internet Policy Statement* that "consumers are entitled to competition among network providers."[7] In order for that aspiration to be realized, however, consumers need access to accurate, adequate information about the limitations of the services offered by their network providers, including the ways in which "network management" may restrict those services.

When a consumer—let's call her Alice—signs up for an "unlimited," high-speed Internet plan, she reasonably expects that she will be entitled to access to the full range of services, applications, and activities that the Internet has to offer. For Alice, that might include surfing the Web and reading email, or videoconferencing, or downloading movies using applications that rely on the BitTorrent protocol (such as that offered by Petitioner Vuze, Inc.), or publishing her own video creations through a file sharing network.

Of course, it may happen that her ISP may not provide Alice with *everything* the Internet has to offer—excessive bandwidth consumption, exposure to viruses, access to phishing web sites, and Alice's ability to send bulk, unsolicited commercial emails come to mind as examples of things that Alice's ISP may want to curtail in the interests of "network management." In each of these cases, Alice's ability to "vote with her wallet" remains an important check on the "reasonableness" of these activities. If, for example, Alice finds that her ISP's policies regarding "excess bandwidth consumption" do not meet her needs, she may want to switch to another provider that offers different practices. In order for this market mechanism to function, however, Alice must have adequate information about the nature and scope of the "network management" being applied by her ISP.[8]

---

[7] *Internet Policy Statement, supra* n. 3, at 3.

[8] This market mechanism also assumes that Alice has alternative ISPs to choose among, a question beyond the scope of this

If her ISP deploys unconventional, non-standard practices for network management, and does not adequately disclose these practices, Alice may well not understand why her applications and services are misbehaving or malfunctioning. For example, if the software application distributed by Petitioner Vuze Inc. were to begin malfunctioning as a result of Comcast's interference with the BitTorrent protocol, Alice might blame the malfunction on Vuze. She might blame it on her own incompetence. She might blame the manufacturer of her computer or the operating system software that runs on it. Any of these misconceptions would mean that she, and other customers like her, would not be able to accurately express their preferences in the marketplace.

This difficulty for Alice and other consumers like her is exacerbated to the extent they are not able to undertake sophisticated network testing in order to diagnose the source of the problem. The Comcast activities that are the subject of this proceeding illustrate this point. Only after weeks of effort and months of consumer complaints were EFF and the Associated Press able to isolate and identify Comcast's interference with P2P traffic.[9] As if this were not bad enough, there is no guarantee that future efforts that ISP undertake in the name of "network management" will be readily diagnosable by independent observers, or that consumer advocacy groups like EFF will have the resources necessary to ferret them out.[10]

B. Transparency Regarding Network Management Serves Competition and Fosters Broadband Deployment.

When consumers lack adequate information on which to base choices among competing products and services, inter-firm competition also suffers, which in turn undermines the role that competition properly plays in encouraging ISPs to constantly improve their broadband networks.

For example, some observers speculate that Comcast has chosen to target P2P traffic for interference because its broadband network infrastructure is comparatively primitive, necessitating Comcast's efforts to conserve scarce upstream bandwidth and limiting its flexibility in deploying alternative options, at least until it is able to upgrade its network infrastructure.[11] If, however, consumers like Alice are kept in the dark about the existence or nature of Comcast's P2P interference efforts, they will be less likely to seek out competitors (assuming other broadband providers have offerings in their area) with more advanced networks and abundant bandwidth, such as Verizon's FiOS service.[12] All else being equal, this will make it less likely that competitors will focus on network improvements that will not serve to differentiate their products in the marketplace.

---

proceeding.

[9] *See* Section VI below for a description of the timeline of events leading up to the confirmation of Comcast's role in BitTorrent interference.

[10] This is particularly true where ISPs either refuse to confirm or actively mislead customers and consumer groups. In this regard, while EFF appreciates AT&T and Verizon's recognition of the value of independent testing by groups like EFF, *see* Comments of AT&T Inc., WC Docket 07-52, filed Feb. 13, 2008, at 33-34; Comments of Verizon and Verizon Wireless, WC Docket 07-52, filed Feb. 13, 2008, at 17, those efforts will be insufficient so long as ISPs remain free to deny, mislead, stonewall, or prevaricate when confronted by evidence of troubling network management practices.

[11] *See* Jim Martin, "The Interaction Between the DOCSIS 1.1/2.0 MAC Protocol and TCP Application Performance," *Proc. Int'l Working Conf. on Performance Modeling & Evaluation of Heterogeneous Networks*, P57/1-10 (2004).

[12] A simple Google search for "Verizon FiOS Comcast BitTorrent" turns up numerous stories of consumers who have switched to Verizon's FiOS service in the wake of revelations regarding Comcast's P2P interference efforts. The fact that Comcast failed to disclose its efforts for months after they were discovered underscores the importance of getting this kind of information into the market.

C. Transparency Regarding Network Management Encourages Innovation.

As the Commission's *Internet Policy Statement* makes clear, one of the strengths of the public Internet is its "open, interconnected nature."[13] Transparency regarding the technological standards on which the Internet is built is part of the foundation of that "open, interconnected nature." Undisclosed deviations from those standards by ISPs, in contrast, erode this valuable characteristic of the public Internet, threatening to Balkanize the network and impede innovation.

Programmers and firms that develop software for the Internet must necessarily follow technical standards. They consult the RFC and Internet Standards documents maintained by the Internet Engineering Task Force (IETF)[14]; they read textbooks written with those standards in mind; they work with software libraries and operating systems that are built around those standards. Comcast's recent interference with P2P traffic is built on subverting a set of those standards, namely, those that define the functions of the so-called TCP "reset" or "RST" packet.[15]

Undisclosed deviations from open Internet standards by ISPs have undesirable consequences for innovators.[16] As discussed above, consumers may incorrectly blame the innovators when their applications or services malfunction, even though the malfunctions are caused by undisclosed "network management" by ISPs. In addition, undisclosed deviations by ISPs from open Internet technical standards will increase entry costs for innovators, forcing them to either negotiate with each ISP or engage in reverse engineering efforts to determine the nature of the deviation and design responses to it—as Petitioner Vuze was forced to do as a result of Comcast's undisclosed P2P interference efforts.[17]

ISPs that clandestinely break from open Internet standards also threaten innovation by undermining the end-to-end principle.[18] The Internet has enabled a cascade of innovations precisely because any

---

[13] *Internet Policy Statement, supra* n. 3, at 3.

[14] For a description of the open Internet standards process, *see* Wikipedia, Internet Standard (http://en.wikipedia.org/wiki/Internet_standard>).

[15] As explained in the EFF Comcast White Paper, *supra* n. 4:

> Reset packets are defined in the TCP specification. *See* RFC 793 / Internet Standard STD 7, http://tools.ietf.org/html/rfc793; *see also* RFC 4614, http://tools.ietf.org/html/rfc4614 (surveying supplements to RFC 793); W. Richard Stevens, *TCP/IP Illustrated Volume 1: The Protocols* 246-250 (1994). According to RFC 793 / STD 7, RST packets were conceived as a means for a computer to signal that the connection no longer exists at its end (*see* RFC 793, Section 3.4); normally, this might be caused by a computer rebooting or by a very large number of dropped packets causing a connection to be closed. They may be used to perform an abortive reset when one party wishes to close a connection quickly and signal an error to the other party; *see* Stevens at 247-8. RST packets are also used in response to a TCP connection attempt to signal that the connection was refused by the destination host, *see* RFC 793 at 69; Stevens at 247.

Importantly, none of these standards contemplate or document the possibility that a RST packet was injected by a third party to the communication as a signal that the connection is consuming too much bandwidth and should slow down or wait and attempt to retry the communication later.

[16] *See, e.g., Vuze Inc. Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators,* WC Docket No. 07-52, Nov. 14, 2007, at 14 (explaining difficulties innovators face from unpredictable network behavior).

[17] *Id.* at 11.

[18] The end-to-end principle holds that the Internet should allow users' computers (the end points) to talk to each other without interference. That way, the functionality of the network is not determined by any of the parties that operate the network's core, but by the users at the ends of each link and the software they choose to run. This ensures both that the best information is available to implement features efficiently, and also that network users have autonomy in determining how their software will communicate. The end-to-end principle was famously originally set out in J.H. Saltzer, D.P. Reed and D.D. Clark, "End-to-End Arguments in System Design", 2 *ACM Transactions on Computer Systems*, 277-288 (1984). RFC

programmer — whether employed by a huge corporation, a startup, or tinkering at home for fun — has been able to create new protocols and applications that conform to open technical standards, without having to obtain permission from anyone. If ISPs are free to selectively deviate from established Internet standards in different ways, the resulting Balkanized patchwork would leave innovators with little choice but to obtain prior permission from major ISPs in order to guarantee that their applications will operate correctly. This creates an innovation environment that favors lengthy negotiations over independent invention, to the ultimate detriment of technical progress.

D. Transparency Regarding Network Management Better Equips Policy-Makers to Evaluate Demands for Further Regulation of Broadband Providers.

Legislators in both the Senate and House of Representatives have introduced bills that would enshrine network neutrality principles in law.[19] The Commission has also conducted proceedings exploring these same questions, with extensive briefing already available in this very Docket. In deciding whether additional legislative or regulatory action is necessary or desirable, these policy-makers will need information about what kinds of "non-neutral" protocol-based or application-based discrimination ISPs are employing. In addition, only if consumers and competitors have access to information about these practices by ISPs will they be able to express their views to these policy-makers. In short, transparency regarding network management practices (particularly where those practices result in application-based or protocol-based discrimination, or where they deviate from established, open Internet standards) is critical if policy-makers are to evaluate whether additional regulatory action is necessary.

E. What Does Transparency Require in the Network Management Context?

The conception of transparency implicit in the idea of "reasonable network management" is not absolute or unbounded. ISPs cannot be expected to make a public announcement each time they make any trivial adjustment to their network infrastructure. As described above, however, without some measure of transparency, important market mechanisms will be disrupted. Even Verizon, which has submitted comments critical of any additional regulatory burden on broadband providers, admits that the broadband consumer needs to "receive information concerning any material and foreseeable limitations on their [broadband] services, including a general description of providers' network management practices that could have such an effect."[20]

The relevant question, then, is how much transparency is required to enable consumers to make informed choices about what products and services to buy. Furthermore, how much transparency is necessary to support the market mechanisms that serve to encourage innovation in protocols and Internet software and effective competition among ISPs?

EFF believes that the answer to these questions can be derived from the *Internet Policy Statement* itself:

1958, Architectural Principles of the Internet, 1996 (<http://www.ietf.org/rfc/rfc1958.txt>), argued that the end-to-end principle was an essential and threatened dimension of the Internet's design; more recent developments are discussed in RFC 3724, The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture, 2004 (<http://www.ietf.org/rfc/rfc3724.txt>). The argument has propagated from technical to legal and policy circles. *See* Lawrence Lessig and Mark A. Lemley, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA Law Review 925 (2001).

[19] *See, e.g.,* Internet Freedom Preservation Act, S. 215, 110th Cong. (2007) (the "Snowe-Dorgan" bill); *see also* Network neutrality in the United States, http://en.wikipedia.org/w/index.php?title=Network_neutrality_in_the_United_States&oldid=190300658 (last visited Feb. 28, 2008) (listing legislative proposals in this area).

[20] *See* Verizon Comments, *supra n.* 10, at 15.

1. In order for a network management practice that would otherwise be inconsistent with any of the Four Principles enunciated in the *Internet Policy Statement* to be deemed "reasonable," it must be adequately disclosed by the ISP; and
2. The disclosure must include enough detail to enable an informed consumer to determine (1) what content, application, service or protocol is likely to be affected, and (2) what consequence is likely to follow.

Network management practices which discriminate with respect to the origin, destination, nature or content of Internet communications are particularly likely to run afoul of Four Principles of the *Internet Policy Statement*. On the other hand, practices that apply equally across the board to Internet traffic are unlikely to implicate the *Internet Policy Statement*, and thus would not require justification as "reasonable network management" under that policy guidance.

For example, where Comcast's P2P interference activities are concerned, these transparency norms would require that Comcast explain (1) that it accords differential treatment to traffic that uses the BitTorrent protocol, thereby affecting applications such as BitTorrent, Azureus, and Vuze; (2) that the consequence for the user of this practice will be interference with "pure seeding" using those applications (uploading a file to another use after the initial download has concluded); and (3) that the practice involves the intentional injection of RST packets into TCP sessions.

Unfortunately, Comcast still has not adequately disclosed this information. Its FAQs, for example, continue to fall short of the mark by failing to inform consumers which applications are likely to be affected, instead vaguely referring to "certain P2P applications" and "peer-to-peer sessions (or sessions using other applications or protocols)."[21] Consumers are left to guess *which* particular P2P applications and protocols may be affected. They are also left to guess *how* those applications may be affected. And while Comcast has (finally) provided more specific details in its comments to the Commission, consumers should not be expected to resort to spelunking in open FCC dockets in order to find them.

III. TRANSPARENCY DOES NOT IMPOSE AN UNDUE BURDEN ON ISPS.

These two transparency principles also address concerns that have been raised by ISPs regarding their other "network management" practices. For example, when it comes to efforts to filter spam from email traffic, a relatively simple disclosure tells consumers what they need to know. *Which* application is affected? Answer: Email services provided by the ISP (and *not* email services provided by others, like Gmail or Hotmail). *How* will it be affected? Answer: Some messages may not be delivered at all, or may be diverted to a special mailbox that can be reviewed by the consumer for false positives (the ISP should specify which of these approaches it uses). ISPs, importantly, would not be required to disclose the precise technical mechanisms and algorithms used in filtering spam.

Many other forms of network management would not have to be disclosed at all, to the extent they do not run afoul of the Four Principles enunciated in the *Internet Policy Statement*. In this regard, Comcast exaggerates when it suggests that "disclosing each of hundreds of tweaks that Comcast and other network operators make to their networks daily – in response to a constantly changing environment – would be practically impossible and would impose significant unjustifiable costs on network operators."[22] For example, if an ISP made adjustments to its network infrastructure by modifying the firmware of its cable modems to more effectively allocate bandwidth for *all* communications, rather than discriminating against any particular application or protocol, there would be no need for specific

[21] *See* Comcast Comments, *supra n.* 1, at Attachment B.

[22] *See* Comcast Comments, *supra n.* 1, at 41.

disclosures. In short, adequate disclosure is relevant only when an ISP invokes "reasonable network management" as an excuse to justify actions that would otherwise be inconsistent with the *Internet Policy Statement*.

IV. TRANSPARENCY NEED NOT COMPROMISE SECURITY.

Similarly, the transparency necessary to facilitate competition and foster innovation need not compromise the legitimate security needs of ISPs. In their efforts to resist calls for adequate disclosure of network management practices, Comcast invokes the specter of malicious hackers:

> [T]here are those actors who would use that level of transparency against Comcast and its subscribers. For example, many of the network management practices that Comcast uses are undertaken specifically to combat malicious uses such as network hacking, viruses, Trojan horses, and spam. Making public every aspect of Comcast's network management practices would not be helpful to the overwhelming majority of Comcast's subscribers—or application or service developers—but would certainly facilitate exactly the kinds of practices that Comcast is trying to defend against.[23]

The transparency principles endorsed above, however, do not require the disclosure of internal technical details that would give a leg up to malicious hackers. ISPs need not disclose every Bayesian spam filter and virus detection rule they apply to their systems. Rather, ISPs should disclose enough information to enable consumers to understand when a particular category of applications or traffic might be targeted for special treatment by the ISP, and what the specific consequences of targeting will be. These *consequences* of network management, after all, will be observable by technical investigation on the customer's computer (in the form of dropped connections or an unanticipated flood of RST packets, for example), and so can hardly be said to be security-critical "secrets" known only to an ISP.[24]

V. ISP RESPONSIVENESS IS ESSENTIAL TO TRANSPARENCY.

In addition to disclosure, transparency requires that ISPs respond honestly to inquiries about practices that may run afoul of the Four Principles set out in the *Internet Policy Statement*. The FCC should therefore clarify that a discriminatory network management practice is not "reasonable" if it is not accompanied by reasonably prompt and accurate responses to questions about problems being caused by that practice.[25]

Whether a network management measure has first come to light as a result of technical research by members of the Internet community, or as a result of some minimal disclosure by the ISP itself, there will be many complicated questions that may subsequently arise. For example, working from guesswork by Comcast subscribers, EFF was able to determine that Comcast was interfering not only with BitTorrent traffic, but also with communications that rely on the Gnutella protocol.[26] Based on Comcast's recent comments to the Commission, it appears that this interference may have been an

---

[23] *Id.*

[24] The reason disclosure is critical is not because customers are unlikely to *notice* the consequences, but rather that he is likely to misunderstand *who is responsible* for any malfunctions that may occur.

[25] The picture Comcast paints of its own best practices, *see* Comcast Comments, *supra n.* 1, at 57-58, suggests that it accepts the importance of responsiveness. Unfortunately, as will be discussed below, it appears that Comcast has not lived up to its own best practices in responding to customers who inquired regarding its interference with BitTorrent traffic.

[26] *See* EFF Comcast White Paper, *supra* n. 4, at 4. LimeWire is the most popular application that relies on the Gnutella protocol, but there are dozens of others, as well.

unintentional byproduct of Comcast's interference with BitTorrent traffic.[27] This underscores the need for an interactive process of disclosure, where ISPs learn from and respond to inquiries from customers, thereby diagnosing any "collateral damage" stemming from their network management practices. Where that collateral damage implicates the Four Principles of the *Internet Policy Statement*, the concept of transparency described above demands that the ISP either correct, or disclose the existence and nature of, the collateral damage in question.

VI. COMCAST HAS FALLEN SHORT WHEN IT COMES TO TRANSPARENCY.

When measured against the standards for transparency described above, Comcast's behavior in connection with its efforts to limit P2P uploading by its customers falls short. After being confronted with reports and inquiries from its customers, Comcast alternately stonewalled its customers and made misleading comments to the press. When pressed by EFF in the wake of continued customer complaints, Comcast continued to provide incomplete or misleading information. Even after being confronted months later by empirical evidence gathered by EFF and the Associated Press, Comcast refused to adequately disclose the nature and scope of the activities that it now claims are justified as a matter of reasonable network maintenance. In fact, not until its comments in this proceeding has Comcast come close to satisfying the norm of transparency implicit in the *Internet Policy Statement*.

EFF urges the Commission to find that Comcast's course of conduct falls short of the norms of transparency that are implicit in the Commission's conception of "reasonable network management" as set out in the *Internet Policy Statement.* By doing so, the Commission can clarify its *Internet Policy Statement* and give guidance to Comcast, other ISPs, and the marketplace regarding the meaning of "reasonable network management."[28]

F. Comcast's Network Management Measures Clearly Implicate the Four Principles.

In light of Comcast's comments and EFF's independent testing, there is now no doubt that Comcast is discriminating among different kinds of Internet traffic based on the protocols used. In particular, Comcast acknowledges that, during periods of network congestion, it uses RST packets to "delay" (*i.e.*, to block, at least temporarily) uploads that use the BitTorrent protocol.[29] EFF's independent testing confirms that Comcast does not interfere with uploads of identical content using other protocols, such as HTTP.[30] The consequences of the discriminatory interventions are complicated, but they are not limited to "delaying" communications.[31]

Protocol-specific discrimination directly implicates the second of the Four Principles, namely that "consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement." Insofar as it may create barriers to entry for next-generation video distribution technologies,[32] Comcast's protocol-specific discrimination also implicates the fourth Principle, namely that "consumers are entitled to competition among network providers, application and service

---

[27] *See* Comcast Comments, *supra n.* 1, at 38 (explaining "Comcast knows of no basis" for complaints regarding interference with Gnutella).

[28] As noted at the outset of these reply comments, EFF expresses no view here on whether the Commission may have the jurisdiction or statutory authority to do more than clarify the meaning of its *Internet Policy Statement*.

[29] *See* Comcast Comments, *supra* n. 1, at 28.

[30] *See* EFF Comcast White Paper, *supra* n. 4, at 3.

[31] *See* EFF Comcast White Paper, *supra* n. 4, at 5.

[32] *See* Vuze Petition, *supra* n.16, at 14-15 (describing threat to competition posed by unfettered ability by ISPs to discriminate against new Internet distribution technologies).

providers, and content providers."

In order to justify its conduct, Comcast maintains that it constitutes "reasonable network management." As discussed above, this catch-all caveat to the Four Principles must implicitly include a norm of transparency, lest the exception effectively swallow the Four Principles altogether.

G. Comcast Failed to Adequately Disclose its Discriminatory Practices.

Credible allegations regarding Comcast's selective interference with certain P2P protocols first came to light in May 2007, when Robb Topolski reported that his informal testing had revealed that RST packets were being forged and selectively injected into his P2P communications with a friend in Brazil.[33]

This revelation quickly garnered widespread attention on the Internet among users of BitTorrent applications. By August 2007, press accounts began appearing on websites that cater to these users, such as TorrentFreak.[34] In response to press inquiries, Comcast made statements that appear in hindsight to be, at the very least, misleading. For example, CNET published the following account after one of its reporters spoke to a Comcast representative:

> When I spoke to Comcast spokesman Charlie Douglas earlier today, he flat-out denied that the company was filtering or "shaping" any traffic on its network. He said the company doesn't actively look at the applications or content that its customers download over the network. … In the rare instances the company has to enforce its policy [against excessive usage], Douglas said that Comcast contacts subscribers to work out the issue. But he firmly reiterated that the company doesn't filter or throttle back traffic.[35]

Similarly, when a reporter from The Register contacted Comcast about the earlier TorrentFreak story, he was also misled:

> Comcast assured us that it was not doing what [TorrentFreak] claims it's doing. Under its current network policy, according to a company spokesman, the company would never block BitTorrent traffic – or traffic related to any other application. The only thing the company would admit to was making polite phone calls to customers guilty of extending some unspecified bandwidth threshold.[36]

Similar flat denials were issued to reporters at WIRED News,[37] The Philadelphia Inquirer,[38] and Silicon Alley Insider,[39] among others.

---

[33] See Robb Topolski, *Comcast is Using Sandvine to Manage P2P Connections* (forum post, available at <http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections>). This post garnered hundreds of responses from interested readers, including many Comcast customers.

[34] *See, e.g., Comcast Throttles BitTorrent Traffic, Seeding Impossible*, TorrentFreak, Aug. 17, 2007 (<http://torrentfreak.com/comcast-throttles-BitTorrent-traffic-seeding-impossible/>).

[35] *See* Marguerite Reardon, *Comcast denies monkeying with BitTorrent traffic*, CNET News, Aug. 21, 2007 (<http://www.news.com/8301-10784_3-9763901-7.html>).

[36] *See* Cade Metz, *Comcast Throttles BitTorrent Users*, The Register, Aug. 22, 2007 (<http://www.theregister.co.uk/2007/08/22/comcast_throttles_BitTorrent_users/>).

[37] *See* Michael Calore, *Comcast Responds: We Don't Block BitTorrent*, Aug. 30, 2007 (<http://blog.wired.com/monkeybites/2007/08/comcast-respond.html>).

[38] Jonathan Berr, *Comcast v. BitTorrent?*, PhillyInc weblog, Sept. 7, 2007 (<http://blogs.phillynews.com/inquirer/phillyinc/2007/09/comcast_vs_BitTorrent_bloggers_1.html>).

[39] *See* Dan Frommer, *Comcast (CMSCA): We Don't Throttle BitTorrent*, Silicon Alley Insider, Aug. 20, 2007

In each of these cases, the reporters were following up on the story originally published by TorrentFreak, which specifically (and correctly) described the selective interference with "pure seeding" by applications that use the BitTorrent protocol. In light of this, even if Comcast's carefully couched denials could be viewed as technically accurate, it is apparent that they were intended to create a misleading picture by undermining the credibility of Mr. Topolski, TorrentFreak, and others who had correctly identified and characterized Comcast's efforts. In the words of the editor of Broadband Reports:

> Comcast is using semantics in their denials…. If you note their responses to most press inquiries, the denials usually say something along the lines of "we do not block access to any applications, including BitTorrent, and do not alter Internet speed." While that's technically correct, they're not really answering the question.[40]

Responding to these press accounts, as well as complaints received directly from Comcast customers, EFF contacted Comcast in September 2007 to specifically inquire about the issue. After a telephone conversation with counsel for Comcast, EFF was left with the following impression, which was posted on EFF's blog immediately after the conversation:

> Comcast assured us that, while it does do some kinds of network management on its residential network, it isn't deliberately blocking, degrading, interfering with, or discriminating against particular protocols or kinds of traffic. (This is consistent with what Comcast told the press in August when these allegations were widely raised.) The company said that it isn't using network management techniques that are designed to disrupt anyone's use of BitTorrent (or any other application).[41]

On October 19, 2007, the Associated Press reported the results of testing that confirmed what TorrentFreak had reported in August.[42] On the same day, EFF published the result of its own independent testing confirming AP's results.[43] Responding to a rising tide of evidence and media attention, Comcast initially reiterated its flat denials.[44] Over the course of several days, however, Comcast began acknowledging that it did "delay" certain traffic in order to "provide all of our users with a good Internet experience."[45] Even at this point, Comcast provided no useful details—it did not confirm which particular protocols it was targeting (BitTorrent), nor under what conditions those protocols would be targeted (only when engaged in "pure seeding" and when faced with local network congestion). Furthermore, it insisted on characterizing complicated interference with applications as "delaying" those applications when in fact a delay was only *sometimes* the outcome.[46]

(<http://www.alleyinsider.com/2007/08/comcast-cmcsa-w.html>).

[40] Quote reported in *Comcast v. BitTorrent?*, *supra* n. 38.

[41] Seth Schoen, *Comcast and BitTorrent*, EFF DeepLinks blog, Sept. 13, 2007 (<http://www.eff.org/deeplinks/2007/09/comcast-and-BitTorrent>).

[42] Peter Svensson, *Comcast Blocks Some Internet Traffic*, SF Gate, Oct. 19, 2007 (<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/10/19/financial/f061526D54.DTL&feed=rss.business>).

[43] Seth Schoen, *EFF tests agree with AP: Comcast is forging packets to interfere with user traffic*, EFF DeepLinks blog, Oct. 19, 2007 (<http://www.eff.org/deeplinks/2007/10/eff-tests-agree-ap-comcast-forging-packets-to-interfere>).

[44] *See, e.g.,* Peter Svensson, *Comcast Blocks Some Internet Traffic*, AP, Oct. 19, 2007 (http://www.msnbc.msn.com/id/21376597/).

[45] *See, e.g.,* Brad Stone, *Comcast: We're Delaying, not Blocking, BitTorrent Traffic*, N.Y. Times Bits blog, Oct. 22, 2007 (<http://bits.blogs.nytimes.com/2007/10/22/comcast-were-delaying-not-blocking-bittorrent-traffic/>).

[46] For an analysis of the consequences of Comcast's RST spoofing against BitTorrent and Gnutella, *see* EFF Comcast White Paper, *supra* n. 4, at 3-5. These are accurate for Comcast's conduct through to January 2008. Comcast does not dispute any

In fact, it appears that it was not until it filed its comments in this proceeding, on February 12, 2008, that Comcast formally acknowledged what its own customers had discovered in May 2007, and independent experts had confirmed in October 2007.[47] And Comcast still has not fully acknowledged or explained the "collateral damage" that was observed in connection with other protocols, such as Gnutella and Lotus Notes.[48]

In other words, nearly 10 months after being confronted about its network management practices, Comcast has only grudgingly disclosed pertinent details regarding the scope and nature of those practices, and only in response to two petitions filed with the Commission. And, as described above, Comcast's "Terms of Use" and "FAQs" still do not adequately disclose to consumers what Comcast has admitted in its FCC comments.

Whatever else "reasonable network management" as used in the Commission's *Internet Policy Statement* might mean, it must at a minimum require more forthright disclosure than this.

VII. CONCLUSION.

For the foregoing reasons, EFF urges the Commission to find that Comcast's course of conduct falls short of the norms of transparency that are implicit in the Commission's conception of "reasonable network management" as set out in the *Internet Policy Statement.* By doing so, the Commission will clarify its *Internet Policy Statement* and give guidance to Comcast, other ISPs, and the marketplace regarding the meaning of "reasonable network management."

Respectfully submitted,

Fred von Lohmann
Peter Eckersley
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

February 28, 2008

---

of the facts in our analysis. With regard to BitTorrent, it simply argues that under "real world" conditions, BitTorrent clients can find a source to download from that isn't on Comcast's network (which is only *sometimes* true); *see* Comcast Comments, *supra* n. 1, at 31-32. The consequences of Comcast's 2007 interference regime on Gnutella were far more radical; *see* EFF Comcast White Paper at 4-5. Comcast tacitly admits that it did not really understand the different consequences of its interference with the BitTorrent and Gnutella protocols; *see* Comcast Comments at 38.

[47] *See* Comcast Comments, *supra n.* 1, at 28.

[48] On Gnutella, *see supra* n. 46. With Regards to Lotus Notes, Comcast offers a carefully worded denial that its interference was *intentional*, *id* at 41-2. The possibility of unintentional interference with untargeted applications simply underscores the need for adequate disclosure and responsiveness.