recharacterized as a form of delay. We are likewise unpersuaded by Comcast's argument that terminating peer-to-peer connections does not equate to blocking access to content because Internet users may upload such content from other sources[205] — whether or not blocking content was Comcast's intent, Comcast's actions certainly had that effect in some circumstances.[206] In any event, the semantic dispute of "delaying vs. blocking" is not outcome determinative here.[207] Regardless of what one calls it, the evidence reviewed above shows that Comcast selectively targeted and terminated the upload connections of its customers' peer-to-peer applications and that this conduct significantly impeded consumers' ability to access the content and use the applications of their choice. These facts are the relevant ones here, and we thus find Comcast's verbal gymnastics both unpersuasive and beside the point.

45. Next, Comcast asserts that even if its practice is discriminatory, it qualifies as reasonable network management.[208] However, experts in the field generally disagree strongly with Comcast's assertion that its network management practices are reasonable. The Internet Engineering Task Force, a repository for the standards and protocols that underlie the functioning of the Internet,[209] has promulgated universal definitions for how the TCP protocol is intended to work.[210] So far in the Internet's history, these standards have created "the equivalent of perfect competition . . . among applications and content . . . with a minimum interference by the network or platform owner."[211] Significantly, Comcast's practices contravene those standards.[212] Comcast's method of sending RST packets to interrupt and terminate TCP connections thus contravenes the established expectations of users and software developers for seamless and transparent communications across the Internet — this practice, known as RST Injection, "violate[s] the expectation that the contents of the envelopes are untouched inside and between Autonomous Systems" and "potentially disrupt[s] systems and applications that are designed assuming the expected behavior of the Internet."[213]

---

[205] *See, e.g.*, Comcast Comments at 33 ("Comcast's network management practices do not, have not, and will not prevent its subscribers from accessing the Internet content of their choice . . . .").

[206] *See supra* para. 42.

[207] *See* Free Press Comments at 36–38 (addressing the semantic debate of whether Comcast's practices are "blocking" or "delaying").

[208] Free Press requests that we declare that a broadband Internet service access provider's selective interference with a particular protocol or application be a per se unreasonable network management practice. *See* Free Press Petition at 28. Because we prefer a more nuanced approach to the issue at this time, we decline Free Press's request.

[209] *See* Internet Engineering Task Force, *available at* http://www.ietf.org/ (last visited July 31, 2008).

[210] *See, e.g.*, RFC 793/Internet Standard STD 7, *available at* http://tools.ietf.org/html/rfc793 (last visited July 31, 2008) (defining the Transmission Control Protocol, or TCP); *see also* Topolski *Ex Parte* at 3 (noting the common set of Internet standards, RFC 5000/STD 1).

[211] Testimony of Lawrence Lessig, C. Wendell and Edith M. Carlsmith Professor of Law, Stanford Law School, Senate Committee on Commerce, Science and Transportation Hearing on "The Future of the Internet," at 2 (Apr. 22, 2008).

[212] *See* Reed Testimony at 3 (citing Sally Floyd, *Inappropriate TCP Resets Considered Harmful*, Internet RFC 3360 (Aug. 2002), *available at* http://www.ietf.org/rfc/rfc3360.txt?number=3360); Free Press Technical *Ex Parte* at 2 (arguing that Comcast's practices deviate from accepted standards); Center for Democracy and Technology Comments at 10; Topolski *Ex Parte* at 3 (arguing that Comcast's practices transgress Internet standards); J.H. Saltzer, D.P. Reed, & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM Transactions on Computer Systems 277 (1984); Lawrence Lessig & Mark A. Lemley, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. Rev. 925, 931 (2001) (arguing that, according to the Internet's design, "communications protocols themselves (the 'pipes' through which information flows) should be as simple and as general as possible"), *cited in* EFF Reply Comments, Attach. at 6. *See generally* Wu, *supra* note 196.

[213] Reed Testimony at 3.

46. As such, numerous experts have condemned Comcast's practice as an unreasonable form of network management. For example, Professor Jon Peha of Carnegie Mellon termed Comcast's practices a "possible case of consumer fraud"[214] and stated that he was "unaware of any technical literature that has proposed that ISPs adopt this particular practice as a way of dealing with congestion, or to use this practice to address any other issue that might be important in the context of 'network management.'"[215] Indeed, he questioned whether Comcast's practices fell "within the realm of network management at all, much less reasonable network management."[216] Professor David Reed of the Massachusetts Institute of Technology said that "[n]either Deep Packet Inspection nor RST Injection" — Comcast uses both to manage its network — "are acceptable behavior."[217] Professor David Clark of the Massachusetts Institute of Technology testified that Comcast was in essence "imposing a value judgment on the consumer, and that is, in the end, looking at your customer and saying 'enemy.'"[218] Professor Tim Wu of Columbia Law School said that "Comcast's methods aren't even in the same league" as reasonable network management and that Comcast was practicing a "form of censorship and filtering rather than management."[219] And Professor Barbara van Schewick of Stanford Law School called Comcast's practices not only unreasonable but also "most harmful for application-level innovation and user choice."[220]

47. Moreover, Comcast's practice selectively blocks and impedes the use of particular applications, and we believe that such disparate treatment poses significant risks of anticompetitive abuse. To the extent that a provider argues that such highly questionable conduct constitutes "reasonable network management," there must be a tight fit between its chosen practices and a significant goal. Accordingly, for Comcast's practice to qualify as reasonable network management, the company's justification for its practice must clear a high threshold.[221] Its practice should further a critically important

---

[214] Peha Comments at 5.

[215] *Id.* at 4.

[216] *Id.*

[217] Reed Testimony at 2. We agree that Comcast's use of Deep Packet Inspection here was unacceptable. However, we make no judgment on the use of this method for different purposes, such as distinguishing legal from illegal content. *See infra* para. 50.

[218] Webcast of Feb. 25, 2008 Broadband Network Management Practices En Banc Public Hearing, Harvard Law School, Cambridge, MA, at 3:31:36–51, *available at* http://www.fcc.gov/realaudio/mt022508v.ram (last visited July 31, 2008).

[219] Testimony of Tim Wu, Professor of Law, Columbia University, First Public En Banc Hearing on Broadband Network Management Practices, at 2 (Feb. 25, 2008).

[220] Testimony of Barbara van Schewick, Assistant Professor of Law, Stanford Law School, Second Public En Banc Hearing on Broadband Network Management Practices, at 3 (Apr. 17, 2008) (van Schewick Testimony); *see also*; Part-15.Org Comments at 6 ("[S]pecifically targeting a specific type of IP protocol would not be in keeping with open-access."); Aaron G. Comments at 2 ("Reasonable traffic shaping . . . only slows [traffic] down or re-queues it to such an extent that the high priority traffic gets the share it needs."); NATOA Comments at 4–5 ("There is no plausible technical or economic reason to suggest that blocking particular applications is a reasonable way to manage a network, particularly because network providers have numerous nondiscriminatory ways to manage the network.").

[221] *Cf. Filing and Review of Open Network Architecture Plans*, CC Docket No. 88-2, Memorandum Opinion and Order, 6 FCC Rcd 7646, 7667–68, para. 47 (1991) (concluding that, in light of the competitive importance of enhanced service providers' access to Bell Operating Companies' operations support systems, it would examine "with a heightened level of scrutiny" the progress reports of those Bell Operating Companies that had not demonstrated significant progress); *Southwestern Bell Corp. v. FCC*, 896 F.2d 1378, 1381 (D.C. Cir. 1990) (upholding the Commission's accounting rules for affiliate transactions, noting that the petitioners themselves "admit that affiliate transactions call for 'heightened regulatory scrutiny'" to protect against possible cost misallocation between regulated and nonregulated activities); *Maine v. Taylor*, 477 U.S. 131, 138 (1986) ("[O]nce a state law is shown to discriminate against interstate commerce 'either on its face or in practical effect,' the burden

interest and be narrowly or carefully tailored to serve that interest. Comcast justifies its practice as a means of easing network congestion, and we will assume without deciding that this is a critically important interest.

48. We next must ask whether Comcast's means are carefully tailored to its interest in easing network congestion, and it is apparent that no such fit exists. As an initial matter, Comcast's practice is overinclusive for at least three independent reasons. First, it can affect customers who are using little bandwidth simply because they are using a disfavored application.[222] Second, it is not employed only during times of the day when congestion is prevalent: "Comcast's current P2P management is triggered . . . regardless of the level of overall network congestion at that time, and regardless of the time of day."[223] And third, its equipment does not appear to target only those neighborhoods that have congested nodes[224] — evidence suggests that Comcast has deployed some of its network management equipment several routers (or hops) upstream from its customers, encompassing a broader geographic and system area.[225] With some equipment deployed over a wider geographic or system area, Comcast's technique may impact numerous nodes within its network simultaneously, regardless of whether any particular node is experiencing congestion. Furthermore, Comcast's practice suffers from the flaw of being underinclusive. A customer may use an extraordinary amount of bandwidth during periods of

---

falls on the State to demonstrate both that the statute 'serves a legitimate local purpose,' and that this purpose could not be served as well by available nondiscriminatory means." (quoting *Hughes v. Oklahoma*, 441 U.S. 322, 336 (1986)).

[222] *See* EFF Reply Comments, Attach. at 7 ("Furthermore, in our testing, we saw no evidence that Comcast was targeting their jamming efforts at customers based on their individual consumption of bandwidth. . . . If Comcast had carefully engineered its interventions to prevent certain users from contributing disproportionately to network con-gestion, we would expect to see jamming only after subscribers consumed large amounts of bandwidth, or when they were participating in large numbers of connections in a short period of time."); Free Press Comments at 35 ("Comcast's actions do not merely affect bandwidth hogs but affect all users of a particular set of protocols."); Letter from Angela M. Simpson, President, Voice on the Net Coalition, to Marlene H. Dortch, Secretary, FCC, at 3–4 (Mar. 14, 2008) (arguing that peer-to-peer VoIP applications generally represent just a "trickle" in today's growing broadband pipes and that Comcast's practice unfairly lumps such applications in with more intensive bandwidth users).

[223] Comcast Technical *Ex Parte* at 5; *see also* Topolski Comments at 4 (Feb. 25, 2008) (citing evidence that Comcast interfered with peer-to-peer connections "regardless of the time of day or night, regardless of the day of the week, and the presumable differences in network congestion during prime time and non-prime time hours of use"); Max Planck Institute Report, *cited in* Free Press Technical *Ex Parte* at 10.

[224] *See* Topolski Letter at 4 ("[I]t needs to be noted that Comcast's installation of Sandvine is at the metropolitan area's aggregation point"); Free Press Technical *Ex Parte* at 11 (citing evidence that Comcast's network management techniques are deployed not at the neighborhood level but "on [the] access routers . . . where the metropolitan area meets 'the backbone'"); Comcast Technical *Ex Parte* at 5 & n.16 (admitting that although "Comcast's network management *generally* occurs at the data node level," "two small [data nodes] near each other may be managed by a single device" (emphasis added)).

[225] This evidence may be summarized roughly as follows: Packets sent over the Internet include TTL or Time-To-Live counters that decrease each time the packet hops to a new destination (*i.e.*, passes another network router). Knowing this, Robert Topolski tested several peer-to-peer TCP connections. RST packets interrupted eighteen of those tests. Using the "trace" application, Topolski determined that each of these interruptions occurred after the connecting packet's TTL had decreased by five, *i.e.*, after that packet had traveled past four separate routers and was headed out of Comcast's network. *See* Comments, "DSLReports: Comcast is using Sandvine to manage P2P Connections" (Aug. 23–24, 2007), *available at* http://www.dslreports.com/forum/r18936691-SandvineBoxFound (last visited July 31, 2008); *see also* Topolski *Ex Parte* at 4–5. That the connecting packets traveled so far before being interrupted suggests that Comcast's network management equipment is not located at the neighborhood level.

network congestion and will be totally unaffected so long as he does not utilize a disfavored application.[226]

49. Moreover, Comcast has several available options it could use to manage network traffic without discriminating as it does. Comcast could cap the average users' capacity and then charge the most aggressive users overage fees.[227] Or Comcast could throttle back the connection speeds of high-capacity users (rather than any user who relies on peer-to-peer technology, no matter how infrequently).[228] Or Comcast can work with the application vendors themselves.[229] As Comcast has touted in this very dispute, negotiations with Pando and BitTorrent, Inc. and other peer-to-peer application companies have advanced the creation of the P4P protocol, which promises "backbone bandwidth optimization" and "improve[d] P2P download performance."[230] Although we do not endorse any of these particular solutions today, they all appear far better tailored to Comcast's basic complaint

---

[226] *See* Payne Reply Comments at 7–8 ("By singling out and controlling particular sources of high volume use to control congestion claimed 'caused' by these sources, Comcast is giving a free ride to all other users during peak periods who contribute equally to congestion . . . ."); Comcast Hearing Remarks at 13 ("Our network management does not 'discriminate' based on . . . the identity of the provider or customer using the P2P protocols . . . ."); Topolski Letter at 5 ("If a Comcast user chooses a Client-Server application to transfer files, such as a web-based browser client or an FTP client, the sessions are allowed unmolested. However, if a Comcast user chooses a Peer-to-Peer application . . . the communications by that application are eventually met with Comcast's forged-injected RST interference . . . ."); *see also* Peha Comments at 4 ("When there is congestion on the beltway (i.e. the ring of highways around Washington DC), it would be ridiculous to assert that this congestion is caused only by the blue cars, even at times when removing the blue cars would end the congestion. Every car that travels on the busiest roadways during peak hours contributes to congestion, and every car suffers from that congestion. Similarly, when the total traffic on a link within Comcast's network is too high, all of the traffic on that link is contributing to congestion.").

[227] We have noted that discriminatory network management is generally an unreasonable response to increased congestion, given the alternatives of "feasible facility improvements or technology-neutral capacity pricing that does not discriminate against subscribers using third-party devices or applications." *See 700 MHz Second Report and Order*, 22 FCC Rcd at 15371, para. 222. Although Comcast rejects a metering solution as incomplete and potentially unviable, Comcast Reply Comments at 17–18, it is a solution embraced by at least one competitor. *See* Time Warner Cable Comments at 24; Brian Stelter, *To Curb Traffic on the Internet, Access Providers Consider Charging by the Gigabyte*, New York Times (June 15, 2008) ("Time Warner Cable, began a trial of 'Internet metering' in one Texas city early this month, asking customers to select a monthly plan and pay surcharges when they exceed their bandwidth limit."), *available at* http://www.nytimes.com/2008/06/15/technology/15cable.html (last visited July 31, 2008); *see also* Information Technology and Innovation Foundation Comments at 9 ("Metered pricing and data caps for broadband services are common in many nations.").

[228] Hughes apparently follows such a practice. *See* Comcast Comments at 21. And one commenter suggests that Comcast's promised non-discriminatory network management practices follow this approach. *See* Letter from George Ou, Senior Analyst, Information Technology and Innovation Foundation, to the Commission, at 9 (July 15, 2008) ("[Comcast's] new system will attempt to fairly distribute bandwidth amongst users instead of amongst protocols so that it can be completely accurate and fair.").

[229] Several commenters recommend just this solution. *See, e.g.*, Soghoian Comments at 2 (If Comcast made "available information on what it considers the peak periods of network traffic . . . it would . . . not be difficult for the authors of BitTorrent applications to modify their programs to query a Comcast server to determine what is the best time to upload/download data.").

[230] Letter from Kathryn A. Zachem, Vice President of Regulatory Affairs, Comcast Corporation, to Marlene H. Dortch, Secretary, FCC, Attach. at 4 (May 16, 2008); *see also id.* at 1 (describing Comcast's efforts with the Distributed Computing Industry Association to come up with best practices for peer-to-peer applications); AT&T Comments at 16–18 (describing AT&T's efforts in the same vein); DCIA Comments at 5–6 (stating that the P4P working group "seeks to create a framework to enable better ISP and P2P coordination" that improves throughput to P2P users, enables ISPs to manage link utilization, reduces the number of links transited by content, and transitions traffic from links having limited capacity links to links with available capacity).

that a "disproportionately large amount of the traffic currently on broadband networks originates from a relatively small number of users."[231]

50. Comcast and several other commenters maintain a continual refrain that "all network providers must manage bandwidth in some manner"[232] and that providers need "flexibility to engage in the reasonable network management practices."[233] We do not disagree, which is precisely why we do not adopt here an inflexible framework micromanaging providers' network management practices.[234] We also note that because "consumers are entitled to access the *lawful* Internet content of their choice,"[235] providers, consistent with federal policy, may block transmissions of illegal content (*e.g.*, child pornography) or transmissions that violate copyright law.[236] To the extent, however, that providers choose to utilize practices that are not application or content neutral, the risk to the open nature of the Internet is particularly acute and the danger of network management practices being used to further anticompetitive ends is strong. As a result, it is incumbent on the Commission to be vigilant and subject such practices to a searching inquiry, and here Comcast's practice falls well short of being carefully tailored to further the interest offered by the company.

51. For all of the foregoing reasons, it is our expert judgment that Comcast's practices do not constitute reasonable network management, a judgment that is generally confirmed by experts in the field.[237] Comcast's practices contravene industry standards and have significantly impeded Internet users' ability to use applications and access content of their choice. Moreover, the practices employed by Comcast are ill-tailored to the company's professed goal of combating network congestion. In sum, the record evidence overwhelmingly demonstrates that Comcast's conduct poses a substantial threat to both the open character and efficient operation of the Internet, and is not reasonable.

52. There is still one more factor we have yet to address: Comcast's failure to disclose its network management practices to its customers. Although we have not adopted (and we decline to adopt today) general disclosure requirements for the network management practices of providers of broadband Internet access services, the anticompetitive harm perpetuated by discriminatory network management practices is clearly compounded by failing to disclose such practices to consumers. Many consumers experiencing difficulty using only certain applications will not place blame on the broadband Internet access service provider, where it belongs, but rather on the applications themselves, thus further

---

[231] Comcast Comments at 25.

[232] *Id.* at 17.

[233] Comcast Reply Comments at 14.

[234] Some commenters cite supposedly similar, or more restrictive, policies regarding peer-to-peer traffic of other entities, such as colleges and universities. *See, e.g.*, Letter from Daniel L. Brenner, Senior Vice President, Law & Regulatory Policy, NCTA, to Marlene H. Dortch, Secretary, FCC, at 1 (July 24, 2008). Other commenters respond that there are additional distinguishing factors in those cases. *See, e.g.*, Letter from Mark Luker, Vice President, EDUCAUSE, to Marlene H. Dortch, Secretary, FCC, at 1–3 (July 25, 2008) (claiming, among other things, different legal and policy implications for management of private networks such as those operated by colleges and universities); Letter from Robert W. Quinn, Senior Vice President-Federal Regulatory, AT&T, to Robert M. McDowell, Commissioner, FCC, at 1–2 (July 25, 2008) (distinguishing between enforceable terms in contracts with end-users and the use of network management technologies, and discussing technological characteristics of mobile wireless networks). Given the case-by-case approach that we set forth in this item, we do not (and need not) opine here on other policies and practices.

[235] *Internet Policy Statement*, 20 FCC Rcd at 14988, para. 4 (emphasis added).

[236] *Cf.* Bryan H. Choi, *The* Grokster *Dead End*, 19 Harv. J. L. & Tech. 393, 410–11 (2006) (arguing that secondary liability suits are a "dead-end" for preventing violations of copyright law).

[237] *See supra* para. 45.

disadvantaging those applications in the marketplace.[238] On the other hand, disclosure of network management practices to consumers in a manner that customers of ordinary intelligence would reasonably understand would enhance the "vibrant and competitive free market . . . for the Internet and interactive computer services"[239] by allowing consumers to compare and contrast competing providers' practices.[240]

53. Comcast's claim that it has always disclosed its network management practices to its customers is simply untrue. Although Comcast's Terms of Use statement may have specified that its broadband Internet access service was subject to "speed and upstream and downstream rate limitations,"[241] such vague terms are of no practical utility to the average customer. Of course there are "limitations" on the speed and bitrate of a customer's Internet connection, but even the best-informed customer would not have inferred from these or Comcast's other terms of service that peer-to-peer protocols were disfavored on Comcast's networks. And although Comcast eventually disclosed some elements of its network management practices to customers, Comcast's first reaction to allegations of discriminatory treatment was not honesty, but at best misdirection and obfuscation.[242] If Comcast actually believed its practices were reasonable, it should not have behaved in this manner. A hallmark of whether something is reasonable is whether a provider is willing to disclose to its customers what it is doing. To the extent that Comcast wishes to employ capacity limits in the future, it should disclose those to customers in clear terms.

54. *Remedy.* — We finally turn to the issue of what action the Commission should take in this adjudicatory proceeding. Section 4(i) of the Act authorizes us to tailor a remedy to "best meet the particular factual situation before [us]."[243] Our overriding aim here is to end Comcast's use of unreasonable network management practices, and our remedy sends the unmistakable message that Comcast's conduct must stop. We note that Comcast has committed in this proceeding to end such practices by the end of this year and instead to institute a protocol-agnostic network management

---

[238] *See* Peha Comments at 5 ("For example, users who saw problems would be likely to incorrectly attribute them to faults in their own hardware or software, even when those problems are entirely caused by Comcast's secret MITM ["man in the middle"] attacks. In addition to P2P users, this is reportedly what happened to users of Lotus Notes, whose traffic was allegedly similarly affected by Comcast practices. Incidents like these can be frustrating, time-consuming, and costly for those affected."); *cf.* James Fallows, *The Connection Has Been Reset*, The Atlantic Monthly (Mar. 2008) (explaining that the Chinese government's Internet management practices "leave the Chinese Internet public unsure about where the off-limits line will be drawn on any given day. . . . In China, the connection just times out. Is it your computer's problem? The firewall? Or maybe your local Internet provider, which has decided to do some filtering on its own? You don't know. 'The unpredictability of the firewall actually makes it more effective,' another Chinese software engineer [said]. 'It becomes much harder to know what the system is looking for, and you always have to be on guard.'").

[239] 47 U.S.C. § 230(b)(2).

[240] *See* van Schewick Testimony at 3 ("[D]isclosed information must provide enough detail to enable customers to make an informed decision and to enable them to adjust their behavior. Comcast's current acceptable use policy falls short of these goals."); EFF Reply Comments at 3–4 (arguing that Comcast's failure to disclose its practices prevented consumers from expressing their preferences by "voting with their wallets").

[241] Comcast Comments at 40.

[242] *See supra* para. 6. Although Comcast and certain other commenters contend that competition among broadband Internet access providers is sufficient to address any concerns regarding network management practices, they do not address the effects of this information asymmetry between the broadband Internet access provider and its customers and competitors. *See, e.g.*, Comcast Comments at 54–55; Comcast Reply Comments at 38–39; Qwest Comments at 5; Verizon Comments at 10. For the same reasons, we likewise are unconvinced that a vocal minority will provide a sufficient constraint on broadband Internet access providers' network management practices. *See, e.g.*, Qwest Comments at 5; Verizon Comments at 5.

[243] *Ashtabula Cable TV, Inc. v. Ashtabula Tel. Co.*, Docket No. 17482, Decision, 17 FCC 2d 113, 119, para. 116 (1969).

technique.[244] We also recognize the need for a reasonable transition period.[245] In light of Comcast's past conduct, however, we believe that the Commission must take action to ensure that Comcast lives up to its promise and will therefore institute a remedy consistent with President Reagan's famous maxim "trust but verify." Specifically, in order to allow the Commission to monitor Comcast's compliance with its pledge, the company must within 30 days of the release of this *Order*: (1) disclose to the Commission the precise contours of the network management practices at issue here, including what equipment has been utilized, when it began to be employed, when and under what circumstances it has been used, how it has been configured, what protocols have been affected, and where it has been deployed; (2) submit a compliance plan to the Commission with interim benchmarks that describes how it intends to transition from discriminatory to nondiscriminatory network management practices by the end of the year; and (3) disclose to the Commission and the public the details of the network management practices that it intends to deploy following the termination of its current practices, including the thresholds that will trigger any limits on customers' access to bandwidth.[246] These disclosures will provide the Commission with the information necessary to ensure that Comcast lives up to the commitment it has made in this proceeding.

55. To the extent that Comcast fails to file the information required above within 30 days of the release of this *Order*, three steps will occur: (1) interim injunctive relief automatically will take effect requiring Comcast to suspend the network management practices described above within 35 days of the release of this *Order*;[247] (2) the Enforcement Bureau will immediately issue an order directing Comcast to show cause why a permanent cease-and-desist order should not be issued against it; and (3) a hearing will be set for thirty days after Comcast's receipt of that order. Similarly, to the extent that Comcast does file the information required above within 30 days of the release of this *Order* but does not follow through on its commitment to end its discriminatory network management practices by the end of the year, three similar steps will occur: (1) interim injunctive relief automatically will take effect requiring Comcast to suspend immediately the network management practices described above; (2) the Enforcement Bureau will immediately issue an order directing Comcast to show cause why a permanent cease-and-desist order should not be issued against it; and (3) a hearing will be set for 30 days after Comcast's receipt of such show-cause order.

---

[244] *See* Letter from Kathryn A. Zachem, Vice President of Regulatory Affairs, Comcast Corporation, to Marlene H. Dortch, Secretary, FCC, at 2 (July 10, 2008) ("We reiterate here that the entire Comcast network will be migrated to [a] new protocol-agnostic management technique by December 31, 2008." (emphasis omitted)); Letter from David L. Cohen, Executive Vice President, Comcast Corporation, to Kevin J. Martin, Chairman, FCC, at 2 (Mar. 28, 2008).

[245] Accordingly, we deny Free Press's request for both a preliminary injunction and a permanent injunction that would require immediate compliance with federal policy, *see* Free Press Complaint at 24–33, as well as various citizen requests for such "immediate" action. *See supra* para. 10.

[246] In the event that Comcast has not finalized the details of the network management practices that it intends to deploy following termination of its current practices in time to meet this deadline, it may instead submit to the Commission a certification to this effect. Should Comcast submit such a certification, Comcast will be required to disclose to the Commission and the public the details of the network management practices that it intends to deploy following the termination of its current practices at least two weeks prior to instituting those new practices.

[247] The Supreme Court affirmed the Commission's authority to impose interim injunctive relief pursuant to section 4(i) in *Southwestern Cable*, *see* 392 U.S. at 181, and the Commission has utilized such authority in the past. *See Time Warner Cable, A Division of Time Warner Entertainment Company, L.P.*, MB Docket No. 06-151, Order, 21 FCC Rcd 8808 (2006); *AT&T Corp. v. Ameritech Corp.*, File No. E-98-41, Memorandum Opinion and Order, 13 FCC Rcd 14508 (1998); *see also Implementation of the Telecommunications Act of 1996; Amendment of Rules Governing Procedures to be Followed When Formal Complaints Are Filed Against Common Carriers*, CC Docket No. 96-238, Report and Order, 12 FCC Rcd 22497, 22566, para. 159 & n.464 (1997) (stating that the Commission has authority under section 4(i) of the Act to award injunctive relief).

56. We invite Free Press and other members of the public to keep a watchful eye on Comcast as it carries out this relief. Using the information provided by Comcast pursuant to this *Order* as well as information submitted by the public, we will closely monitor the company's network management practices.[248] Accordingly, we will not terminate this proceeding but rather retain jurisdiction over this matter.

IV. ORDERING CLAUSES

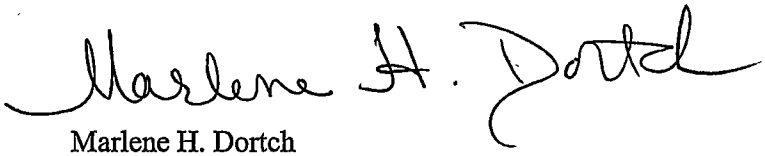
57. Accordingly, IT IS ORDERED that, pursuant to sections 1, 2(a), 4(i), 4(j), 201(b), 230(b), 256, 257, 303(r), 403, and 601 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152(a), 154(i), 154(j), 201(b), 230(b), 256, 257, 303(r), 403, 521, and section 706 of the Telecommunications Act of 1996, 47 U.S.C. § 157 nt, the complaint filed by Free Press against Comcast Corporation on November 1, 2007 IS GRANTED TO THE EXTENT HEREIN DESCRIBED AND OTHERWISE DENIED.

58. IT IS FURTHER ORDERED that, pursuant to sections 1, 2(a), 4(i), 4(j), 201(b), 230(b), 256, 257, 303(r), 403, and 601 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152(a), 154(i), 154(j), 201(b), 230(b), 256, 257, 303(r), 403, 521, section 706 of the Telecommunications Act of 1996, 47 U.S.C. § 157 nt, and section 1.2 of the Commission's rules, 47 C.F.R. § 1.2, the petition for a declaratory ruling filed by Free Press on November 1, 2007 IS GRANTED TO THE EXTENT HEREIN DESCRIBED AND OTHERWISE DENIED.

59. IT IS FURTHER ORDERED that, pursuant to sections 1, 2(a), 4(i), 4(j), 201(b), 230(b), 256, 257, 303(r), 403, and 601 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152(a), 154(i), 154(j), 201(b), 230(b), 256, 257, 303(r), 403, 521, and section 706 of the Telecommunications Act of 1996, 47 U.S.C. § 157 nt, Comcast must take the steps set forth in paragraph 54 of this *Memorandum Opinion and Order*.

60. IT IS FURTHER ORDERED that this *Memorandum Opinion and Order* SHALL BE EFFECTIVE upon release.

FEDERAL COMMUNICATIONS COMMISSION



Marlene H. Dortch
Secretary

[248] We decline, at this time, to assess any forfeitures against Comcast, cognizant of concerns that have been expressed about fining Comcast in our first adjudication in this area. *See supra* para. 34.

APPENDIX

List of Commenters

***Broadband Industry Practices*, WC Docket No. 07-52, Comment Sought on Petition for Declaratory Ruling Regarding Internet Management Policies, Public Notice, 23 FCC Rcd 340 (WCB 2008).**

Commenter	Abbreviation
American Homeowners Grassroots Alliance	AHGA
American Library Association	ALA
AT&T Inc.	AT&T
Richard Bennett	Bennett
Center for Democracy & Technology	CDT
Comcast Corporation	Comcast
Competitive Enterprise Institute	CEI
Computer & Communications Industry Association	CCIA
CTIA f--f The Wireless Association	CTIA
Discovery Institute	Discovery Institute
Distributed Computing Industry Association	DCIA
Embarq	Embarq
Dean Fox	Fox
Fiber-to-the-Home Council	FTTH Council
Free Press; Public Knowledge; Media Access Project; Consumer Federation of America; Consumers Union; New America Foundation; Participatory Culture Foundation	Free Press
Free State Foundation	Free State
Frontier Communications	Frontier
Laurence Brett Glass d/b/a LARIAT	LARIAT
David Gerisch	Gerisch
Global Crossing North America, Inc.	Global Crossing
Hands off the Internet	Hands off the Internet
Health Tech Strategies, LLC	HTS
Independent Telephone & Telephone Communications Alliance	ITTA
Information Technology and Innovation Foundation	ITIF
Information Technology Association of America	ITAA
Institute for Policy Innovation	IPI
Danny Ray Jackson	Jackson
Labor Council for Latin American Advancement	LCLAA
Nickolaus E. Leggett	Leggett
Curtis L. Lowery, M.D., University of Arkansas for Medical Sciences	Lowery
Brad Lindaas *et al.*, Northwestern University Students for Net Neutrality	Lindaas *et al.*
National Association of Realtors	Nat'l Ass'n of Realtors
National Association of State Utility Consumer Advocates	NASUCA
National Association of Telecommunications Officers and Advisors	NATOA
National Black Chamber of Commerce	NBCC
National Cable and Telecommunications Association	NCTA
National Grange of the Order of Patrons of Husbandry	National Grange
National Public Safety Telecommunications Council	NPSTIC
National Telecommunications Cooperative Association	NTCA
NBC Universal Inc.	NBC Universal

New York Public Service Commission	NYPSC
The OASIS Institute	OASIS
Open Internet Coalition	Open Internet Coalition
Organization for the Promotion and Advancement of Small Telecommunications Companies	OPASTCO
George Ou	Ou
Part-15 Organization	Part-15.ORG
Progress and Freedom Foundation	PFF
Qwest Communications International, Inc.	Qwest
Recording Industry Association of America	RIAA
SafeMedia Corporation	SafeMedia
Small Business and Entrepreneurship Council	SBE Council
Christopher Soghoian	Soghoian
Sony Electronics, Inc.	Sony
Telecommunication Industry Association	TIA
Time Warner Cable, Inc.	Time Warner
Steven Titch, The Reason Foundation	Titch
Michael Trausch	Trausch
Joseph Tucek	Tucek
U.S. Chamber of Commerce	US Chamber of Commerce
United States Internet Industry Association	USIIA
United States Telecom Association	USTelecom
Verizon and Verizon Wireless	Verizon
Vonage Holdings Corp.	Vonage
Vuze, Inc.	Vuze
Women Impacting Public Policy	WIPP
Wireless Communications Association International, Inc.	WCA

Reply Commenter	**Abbreviation**
Beth Ahern	Ahern
Ad Hoc Telecom Manufacturer Coalition	AdHoc
Advanced Communications Law & Policy Institute at New York Law School	ACLPI
American Legislative Exchange Council, Telecommunications & Information Technology Task Force	ALEC
AT&T Inc.	AT&T
Richard Bennett	Bennett
BeSafe Technologies Inc.	BeSafe
Center for Democracy & Technology	CDT
Christian Coalition of America; the CP80 Foundation; Enough is Enough; and Stop Child Predators	Christian Coalition *et al.*
Cisco Systems, Inc.	Cisco
CTIA – The Wireless Association	CTIA
Comcast Corporation	Comcast
Computer & Communications Industry Association	CCIA
Consumer Federation of America and Consumers Union	CFA/CU
Electronic Frontier Foundation	EFF
Free Press; Public Knowledge; Media Access Project; Consumer Federation of America; Consumers Union; New America Foundation; Participatory Culture Foundation	Free Press

Aaron G.	Aaron G.
Hands Off the Internet	Hands Off the Internet
Sean Kass	Kass
Motion Picture Association of America	MPAA
The National Grange of the Order of Patrons of Husbandry	National Grange
New Jersey Division of Rate Counsel	NJ Rate Counsel
National Association of State Utility Consumer Advocates	NASUCA
National Black Chamber of Commerce; Labor Council for Latin American Advancement; Latinos in Information Sciences and Technology Association; League of Rural Voters; National Black Justice Coalition; National Council of Women's Organizations; and National Congress of Black Women	NBCC Coalition
NBC Universal, Inc.	NBC Universal
Barry Payne	Payne
The Progress & Freedom Foundation	PFF
Recording Industry Association of America	RIAA
Songwriters Guild of America	SGA
Sprint Nextel Corporation	Sprint Nextel
Anthony Tarsia	Tarsia
Telecommunications for the Deaf and Hard of Hearing, Inc.	TDI
Telecommunications Industry Association	TIA
S. Michael Telford	Telford
Time Warner Cable Inc.	Time Warner
Robert M. Topolski	Topolski
U.S. Chamber of Commerce	US Chamber of Commerce
U.S. Distance Learning Association	USDLA
United States Hispanic Leadership Institute	USHLI
United States Telecom Association	USTelecom
Verizon and Verizon Wireless	Verizon
Viacom Inc.	Viacom
Vonage Holdings Corp.	Vonage
Vuze, Inc.	Vuze

STATEMENT OF CHAIRMAN KEVIN J. MARTIN

Re: Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices, File No. EB-08-IH-1518, WC Docket No. 07-52

Would it be OK if the post office opened your mail, decided they didn't want to bother delivering it, and hid that fact by sending it back to you stamped "address unknown – return to sender"? Or would it be OK, when someone sends you a first class-stamped letter, if the post office opened it, decided that because the mail truck is full sometimes, letters to you could wait, and then hid both that they read your letters and delayed them?

Unfortunately, that is exactly what Comcast was doing with their subscribers' Internet traffic.

Last year, some broadband subscribers complained to the FCC that Comcast was blocking and delaying their Internet traffic. Our investigation, and the findings of several widely respected engineers, confirmed the complaints. Comcast was delaying subscribers' downloads and blocking their uploads. It was doing so 24/7, regardless of the amount of congestion on the network or how small the file might be. Even worse, Comcast was hiding that fact by making effected users think there was a problem with their Internet connection or the application.

Today, the Commission tells Comcast to stop, and to disclose to its subscribers how it is going to manage traffic on a going forward basis. We therefore take another important step to ensure that all consumers have unfettered access to the Internet.

Over the past decade, the Internet has had a powerful impact on the economy and on the lives of American citizens. Thanks in large part to the deregulatory approach the Commission has employed, we have witnessed the fruits of increased innovation, entrepreneurship, and competition that the Internet has helped deliver. As policymakers, we have a duty to preserve and promote the vibrant and open character of the Internet while maintaining infrastructure companies' incentive to invest in providing faster broadband to more people.

The framework we adopt today will enable us to achieve this balance, and will send a message to the industry that bad actors will be punished. This is the same framework and approach that I proposed in my April testimony before the Senate Committee on Science, Commerce, and Transportation which is attached as an Appendix to this statement.[1]

We begin by affirming that the Commission can and will enforce the principle that consumers should be able to access any content and any application. This should come as no surprise. Three years ago the Commission declared that it would not hesitate to act if faced with evidence that a provider was violating this principle by blocking consumer access to content or applications. Last year the current Commission unanimously reiterated that we have "the ability to adopt and enforce the net neutrality principles ... announced in the Internet Policy Statement." Regardless of the dissenting Commissioners' intentions at the time, or their personal preference for a rulemaking now, the full Commission clearly put broadband operators on notice that we were ready, willing, and able to enforce the principles.

In fact, we've said this several times, including specifically telling Comcast. In the 2006 *Adelphia* Order, which the dissenting Commissioners voted for, the Commission clearly indicated it

[1] Written Statement of the Honorable Kevin J. Martin, Chairman, Federal Communications Commission, Before the United States Senate Committee on Commerce, Science and Transportation (April 22, 2008) (attached as an Appendix).

would act on any complaints that it received about blocking or degrading Internet content. Specifically, the Commission stated:

> "If in the future evidence arises that any company is willfully blocking or degrading Internet content, affected parties may file a complaint with the Commission."

In conducting such an analysis, we consider a variety of factors. The Commission considers whether the network management practice is intended to distinguish between legal and illegal activity. The Commission's network principles only recognize and protect user's access to legal content. The sharing of illegal content, such as child pornography or content that does not have the appropriate copyright, is not protected by our principles. Similarly, applications that are intended to harm the network are not protected.

The Commission also considers whether the network service provider adequately disclosed its network management practices. A hallmark of whether something is reasonable is whether an operator is willing to disclose fully and exactly what they are doing. Consumers need proper disclosure so that they can make informed decisions when purchasing broadband service.

Finally, if legal content is arbitrarily degraded or blocked, and the defense is "network management," the broadband operator must show that its network management practice is reasonable. We will look at whether it furthers an important interest and is carefully tailored to serve that interest. Also, the practice should be disclosed to consumers so that they can make informed decisions when purchasing broadband service.

Applying this framework, we find that it was unreasonable for Comcast to discriminate against particular Internet applications, including BitTorrent.

While Comcast claimed its intent was to manage congestion, the evidence told a different story:

- Contrary to Comcast's claims, they blocked customers who were using very little bandwidth simply because they were using a disfavored application;
- Contrary to Comcast's claims, they did not affect other customers who were also using an extraordinary amount of bandwidth even during periods of peak network congestion as long as he wasn't using a disfavored application;
- Contrary to Comcast's claims, they delayed and blocked customers using a disfavored application even when there was no network congestion;
- Contrary to Comcast's claims, the activity extended to regions much larger than where it claimed congestion occurred.

In short, they were not simply managing their network; they had arbitrarily picked an application and blocked their subscribers' access to it.

Comcast's lack of disclosure about its network management practices compounded the harm. Customers that experience unexpected problems with their connections may blame the connection or application. This is particularly troubling when the application is used to provide services that compete with the broadband operator's own services. Indeed, when faced with a similar situation with Internet telephony, we took quick action to stop a telecommunications carrier from blocking competitive VoIP

providers.

Consumers demand, and deserve, better.

Our action today is not about regulating the Internet. Indeed, I have consistently opposed calls for legislation or rules to impose network neutrality. Like many other policy makers and members of Congress, I have said such legislation or rules are unnecessary, because the Commission already has the tools it needs to punish a bad actor. Instead, we take a cautious approach. Adopting broad regulations in this area could have unintended consequences that could stifle technological innovation. By acting on the complaints that we receive, we are able to deal with actual problems and avoid creating others.

That is what we do today. The specific practice Comcast was engaging in has been roundly criticized and not defended by a single other broadband provider.

If we aren't going to stop a company that is looking inside its subscribers' communications (reading the "packets" they send), blocking that communication when it uses a particular application regardless of whether there is congestion on the network, hiding what it is doing by making consumers think the problem is their own, and lying about it to the public, what would we stop? Failure to act here would have reasonably led to the conclusion that new legislation and rules are necessary.

We do not address pricing, unbundling, or other economic regulation.

We do not tell providers how to manage their networks. They might choose, for instance, to prioritize voice-over-IP calls. In analyzing whether Comcast violated federal policy when it blocked access to certain applications, we conduct a fact-specific inquiry into whether the management practice they used was reasonable. Based on many reasons, including the arbitrary nature of the blocking, the lack of relation to times of congestion or size of files, and the manner in which they hid their conduct from their subscribers, we conclude it was not.

We do not limit providers' efforts to stop congestion. We do say providers should disclose what they are doing to consumers.

We make clear that network operators can block any illegal content or applications that are intended to harm the network. The Order makes clear, for instance, that providers can block child pornography or pirated video and music. Indeed, blocking illegal content could reduce bandwidth congestion.

While concluding that the conduct at issue violates our policy was an obvious step, our action today is nevertheless critically important.

I am pleased that Comcast has reached an agreement with the company BitTorrent and has committed to implement a new "protocol-agnostic" management technique by the end of the year. And I note that we have decided not to issue a fine. But contrary to some claims, Comcast's agreement with the company BitTorrent did not obviate the need for us to act today.

First, BitTorrent was not a party to the proceeding. Consumer groups brought the complaint – not BitTorrent – and they and Comcast have not settled. As a basic issue of administrative law, we need to resolve the complaint. Comcast's agreement with a single company that uses the peer-to-peer protocol is not a substitute for addressing the consumer groups' complaint.

Second, it is important for the Commission to establish the important precedent that we will stop the bad actors. We establish a clear framework for how we will conduct our fact-intensive inquiries if

situations arise in the future. If we had declined to act, as the dissenting Commissioners would have preferred, we would have provided certainty that broadband operators can block access and hide their actions from their own customers.

Third, we need to protect consumers' access. While Comcast has said it would stop the arbitrary blocking, consumers deserve to know that the commitment is backed up by legal enforcement.

Finally, particularly given the previous obfuscation Comcast engaged in to date, it is important that we require Comcast to respond to many still-unanswered questions about their new management techniques:

- What exactly do they mean by a "protocol agnostic" management technique?
- Will there be bandwidth limits?
- If so, what will they be?
- Will they be hourly? Monthly?
- How will consumers know if they are close to a limit?
- If a consumers exceeds a limit, is his traffic slowed? Is it terminated? Is his service turned off?

The Commission needs to understand the answers. Perhaps more importantly, Comcasts' subscribers deserve to know the answers.

These unanswered questions seem inconsistent with the disclosures that even the dissenting Commissioners agree are necessary.

The dissenters argue that the Commission should have conducted an investigation to find out the answers to these questions. We did. Our Enforcement Bureau sent Comcast a letter asking the company to respond to the allegations in the complaint and Comcast replied. Moreover, the Commission sought comment on petitions by Vuze and Free Press, which asked the Commission to rule on the same conduct at issue in the complaint and received more than 6,500 comments in response. In addition, the Commission held two public hearing on the complaint and the petitions. In total, the record contains more than 60,000 pages filling 15 banker boxes.

The fact that Comcast still has not come forward and disclosed the true nature of its network management practices, despite numerous opportunities to do so, cannot justify inaction on the complaint. Given the voluminous record evidence that Comcast engaged in unreasonable network management practices, it was incumbent upon us to order Comcast to stop the practices and disclose them to us. That is precisely what we are doing today.

In sum, by applying the framework we adopt today, the Commission will remain vigilant in protecting consumers' access to content on the Internet. Subscribers should be able to go where they want, when they want, and generally use the Internet in any legal means. When providers engage in practices truly designed to manage congestion, not cripple a potential competitive threat, they should not be afraid to disclose their practices to consumers.

APPENDIX

Written Statement
Of

The Honorable Kevin J. Martin
Chairman
Federal Communications Commission

Before the
United States Senate
Committee on Commerce, Science and Transportation

April 22, 2008

APPENDIX

Good morning Chairman Inouye, Vice Chairman Stevens, and Members of the Committee. Thank you for inviting me here today to provide my thoughts on the future of the Internet and the Commission's current role on some of the issues being discussed today.

Over the past decade, the Internet has had a powerful impact on the economy and on the lives of American citizens. We have witnessed the fruits of increased innovation, entrepreneurship, and competition that this technology has helped deliver. As policymakers, any rules of the road in this area must maintain an open and dynamic Internet that will allow it to continue to be an engine of productivity and innovation that benefits all Americans.

I. FCC PRINCIPLES PROTECTING CONSUMER ACCESS TO THE INTERNET

The Commission has a duty to preserve and promote the vibrant and open character of the Internet as the telecommunications marketplace enters the broadband age. In 2005, the Commission adopted an Internet Policy Statement containing four principles. The Commission's goal was to clarify how it would evaluate broadband Internet practices on a going forward basis.

Specifically, the Commission established the following principles:

To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,

- Consumers are entitled to access the lawful Internet content of their choice;
- Consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement;
- Consumers are entitled to connect their choice of legal devices that do not harm the network;

APPENDIX

- Consumers are entitled to competition among network providers, application and service providers, and content providers.

The Commission explicitly noted that these principles were subject to reasonable network management.

The Commission was seeking to protect consumers' access to the lawful online content of their choice. The intent of these principles was to foster the creation, adoption and use of broadband Internet content, applications, and services, and to ensure that consumers benefit from that innovation.

II. FCC's ROLE IN PROTECTING CONSUMERS AND ENFORCING OUR PRINCIPLES

As the expert communications agency, it was appropriate for the Commission to adopt, and it is the Commission's role to enforce, this Internet Policy Statement.

In fact, the Supreme Court in its Brand X decision specifically recognized the Commission's ancillary authority to impose regulations as necessary to protect broadband internet access.

I do not believe any additional regulations are needed at this time. But I also believe that the Commission has a responsibility to enforce the principles that it has already adopted. Indeed, on several occasions, the entire Commission has reiterated that it has the authority and will enforce these current principles.

For example, in 2006 when I appeared before this Committee, then Chairman Stevens asked me whether the Commission had the existing authority to take action if a problem developed. And I

APPENDIX

responded that the Commission had authority under Title I to enforce consumers' access to the internet.

Moreover, almost exactly one year ago, the Republican Majority of the Commission, with the Democrat Commissioners concurring, committed to enforcing our existing principles and the policy statement. Specifically, in April 2007, the Commission expressly stated:

> The Commission, under Title I of the Communications Act, has the ability to adopt and enforce the net neutrality principles it announced in the Internet Policy Statement. The Supreme Court reaffirmed that the Commission "has jurisdiction to impose additional regulatory obligations under its Title I ancillary jurisdiction to regulate interstate and foreign communications." Indeed, the Supreme Court specifically recognized the Commission's ancillary jurisdiction to impose regulatory obligations on broadband Internet access providers.[1]

Finally, the Commission has already taken enforcement action in response to other complaints. In the Madison River complaint, the Commission ordered a telephone company to stop blocking VoIP calls.

Contrary to some public claims about Commission's approach generally, for the Commission to take enforcement action against a telephone company for blocking and degrading a particular application but refuse to pursue enforcement action against a cable company blocking or degrading a particular application would unfairly favor the cable industry.

I believe that the Commission must remain vigilant in protecting consumers' access to content on the internet. Thus, it is critically important that the Commission take seriously and respond to complaints that are filed about arbitrary limits on broadband access and potential violations of our principles. Indeed, I have publicly stated that the Commission stands ready to enforce this policy statement and protect consumers' access to the internet.

APPENDIX

III. FRAMEWORK FOR EVALUATING REASONABLE NETWORK MANAGEMENT COMPLAINTS

The Commission should address issues of appropriate network management using a consistent framework. There are several factors that I believe the Commission should use when analyzing complaints and concerns about network management practices by broadband operators.

First, the Commission should consider whether the network management practices are intended to distinguish between legal and illegal activity. The Commission's network principles only recognize and protect user's access to legal content. The sharing of illegal content, such as child pornography or content that does not have the appropriate copyright, is not protected by our principles. Similarly, applications that are intended to harm the network are not protected.

Second, the Commission should consider whether the network service provider adequately disclosed its network management practices. A hallmark of whether something is reasonable is whether an operator is willing to disclose fully and exactly what they are doing.

Adequate disclosure of the particular traffic management tools and techniques -- not only to consumers but also to the designers of various applications and entrepreneurs – is critical.

Application designers need to understand what will and will not work on a particular network. For example, does an application developer know that the operator may actually insert reset packets during a session masking the network operator's identity?

[1] *Broadband Industry Practices*, WC Docket No. 07-52, Notice of Inquiry, 22 FCC Rcd 7894, 7896, para. 4 (2007) (internal footnotes omitted).

APPENDIX

Consumers must be fully informed about the exact nature of the service they are purchasing and any potential limitations associated with that service. For example, has the consumer been informed that certain applications used to watch video will not work properly when there is high congestion?

Particularly as broadband providers begin providing more complex tiers of service, it's critical to make sure that consumers understand whether broadband network operators are able to deliver the speeds of service that they are selling. For example, if Internet access is sold as an unlimited service, do consumers understand that if they use too much of it they can still be cut-off?

Finally, the Commission should consider whether the network management technique arbitrarily blocks or degrades a particular application. Is the network management practice selectively identifying particular applications or content for differential treatment? If so, I believe that we should evaluate the practices with heightened scrutiny, with the network operator bearing the burden of demonstrating that the particular practice furthered an important interest, and that it was narrowly tailored to serve that interest.

Such an approach would not mean that any action taken against a particular application would automatically be a violation. Rather, it would trigger a more searching review of both the particular concern and whether that network management solution was tailored to resolve the particular harm identified to the network in as narrow a manner as possible.

In a manner similar to the way in which restrictions on speech are analyzed, network management solutions would need to further a compelling or at least an important/legitimate interest and would need to be tailored to fit the exact interest. Such practices should not be overly broad in their application so that they become over or under inclusive. For example, if the concern is about stopping certain illegal

APPENDIX

content, a network provider should not block a particular application to all users if that application transmits both legal and illegal content.

Such an analysis would recognize the importance of legitimate network management techniques while giving the Commission the framework to analyze carriers actions on a case-by-case basis. As we move into an era in which network operators are taking particularized actions against individual applications and content, the Commission should evaluate such practices under sufficient scrutiny to ensure that whatever actions the operators are taking are actually furthering a legitimate purpose and are narrowly tailored to serving that legitimate purpose.

IV. PENDING COMCAST COMPLAINT

Consumers have alleged that certain operators, and specifically Comcast, are blocking and/or degrading consumers' access to the Internet by distinguishing between applications.

The Commission has heard from several engineers and technical experts who have raised questions regarding the network management techniques used by Comcast for peer-to-peer traffic.

The Commission is still investigating these complaints and we have not yet determined whether the actions violated our principles protecting consumer access to the Internet. However, Comcast appears to have utilized Internet equipment from Sandvine or something similar that is widely known to be a relatively inexpensive, blunt means to reduce peer-to-peer traffic by blocking certain traffic completely. In contrast, more modern equipment can be finely tuned to slow traffic to certain speeds based on various levels of congestion.

APPENDIX

Specifically, this equipment (1) blocks certain attempts by subscribers to upload information using particular legal peer-to-peer applications by pretending to be the subscriber's computer and falsifying a "reset" packet to end the communication, and (2) degrades the corresponding attempts to download information using the same peer-to-peer applications.

Based on the testimony we have received thus far, I think it is important to clarify a few points.

Contrary to some claims, it does not appear that cable modem subscribers had the ability to do anything they wanted on the Internet. Specifically, based on the testimony we have received thus far, some users were not able to upload anything they wanted and were unable to fully use certain file sharing software from peer-to-peer networks.

Contrary to some claims, it does not appear this network management technique is "content agnostic." Indeed, Comcast has publicly stated that it will migrate to a "protocol" (content) agnostic approach to traffic management in the future, and thus conceded that the techniques currently in use are not "content agnostic."

Contrary to some claims, it does not appear that this technique was used only to occasionally delay traffic at particular nodes suffering from network congestion at that time. Indeed, based on the testimony we have received thus far, this equipment is typically deployed over a wider geographic or system area and would therefore have impacted numerous nodes within a system simultaneously. Moreover, the equipment apparently used does not appear to have the ability to know when an individual cable segment is congested. It appears that this equipment blocks the uploads of at least a large portion of subscribers in that part of the network, regardless of the actual levels of congestion at that particular time.

APPENDIX

Finally, contrary to some claims, it is not clear when they will actually stop using their current approach. They claim that they will deploy this new solution by the end of the year but it is unclear whether they will be finished deploying their solution or just starting that migration. Indeed the question is not when they will begin using a new approach but if and when they are committing to stop using the old one.

V. NEXT STEPS

As the Commission continues its investigation into the complaints before it, the most important and first step that we can take in fulfilling our responsibility is to make sure that we are fully informed. At the very least, we need to obtain greater information to more fully understand what is happening and what impact operators' actions are having so that we may better evaluate the reasonableness of any network management practices at issue.