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

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

COMMENTS OF ELECTRONIC FRONTIER FOUNDATION
January 14, 2010

TABLE OF CONTENTS

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

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

COMMENTS OF ELECTRONIC FRONTIER FOUNDATION
January 14, 2010

The Electronic Frontier Foundation (EFF) submits the following comments in response to the Commission's October 22, 2009, Notice of Proposed Rulemaking (NPRM), FCC No. 09-93, in the above-captioned proceedings.

I. ABOUT EFF

EFF is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in technology, law, policy and standards. With over 14,000 dues-paying members and over 74,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

EFF has campaigned both in the United States and abroad against ill-considered efforts to block, filter, or degrade access for citizens to the public Internet. EFF is actively developing and promoting technological tools which consumers and activists can use to test their broadband Internet connections to see if Internet access service providers are interfering with the traffic to and from users' computers.[1] EFF was among the first to independently test and discover the

[1] EFF, Test Your ISP.

precise nature and scope of Comcast's 2007 interference with BitTorrent and potentially other peer-to-peer applications.[2]

II. INTRODUCTION AND SUMMARY

As the NPRM recognizes, the Internet has evolved to be the vast platform for commerce, innovation, and free speech that it is today because of its "openness, and the transparency of its protocols."[3] These characteristics have enabled innovators and content creators to experiment without first having to beg permission from providers of broadband Internet access service (ISPs).[4] This freedom to innovate has been crucial to the explosion of new applications and services on the Internet, which in turn have made the Internet a global platform for free expression and commerce of every kind.

The Commission is right to be concerned that the openness and transparency of the Internet may be in jeopardy. Already, we have seen some troubling examples of protocol-based discrimination by ISPs. In 2005, Madison River Communications selectively blocked "voice-over-IP" (VoIP) services that could compete with its wireline telephone services.[5] More recently, Comcast was caught clandestinely using technology to selectively interfere with applications using the BitTorrent protocol.[6] Other ISPs have experimented with similar technologies, often

---

[2] *See* EFF White Paper, Packet Forgery By ISPs: A Report on the Comcast Affair (November 2007).

[3] October 22, 2009, Notice of Proposed Rulemaking (NPRM), FCC No. 09-93 (hereinafter "NPRM") at ¶ 3.

[4] These comments will use the more common term "ISP" or "Internet service provider" as a synonym for "provider of broadband Internet access service" as that term is used in the NPRM. *See* NPRM ¶ 55.

[5] Madison River Communications, File No. EB-05-IH-0110, Order, 20 FCC Rcd 4295 (EB 2005).

[6] Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's

without adequate disclosure to consumers or innovators. If protocol- and application-based discrimination were to become more common, creators would have to seek advance permission from ISPs, and perhaps pay a premium or be blocked from providing new tools to customers. These hurdles would pose a serious threat to innovation on the Internet.

EFF is also concerned that content-based discrimination may be looming on the horizon. The entertainment industry, for example, has been pressing ISPs to implement network-based measures to address the problem of online copyright infringement.[7] Experience suggests that these technologies are likely to be overbroad, ineffective, expensive, and impede innovation.[8]

While EFF shares many of the Commission's concerns regarding the preservation of the characteristics that have made the Internet so successful, EFF also believes that market competition should be the first and preferred line of defense for innovators and consumers against abusive ISP practices. But, because most Americans have only one or two realistic choices for residential broadband, normal market mechanisms may not effectively prevent dominant ISPs from adopting policies that undermine the openness that has so far characterized the Internet.[9] These companies may have economic incentives to capitalize on their ownership of the transmission infrastructure by not only selling Internet access to consumers at higher prices, but also by selling access to those customers to a select set of partners, or by privileging their

---

Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management," File No. EB-08-IH-1518, WC Docket No. 07-52, Memorandum Opinion and Order, 23 FCC Rcd 13028 (2008) (hereinafter *Comcast Network Management Practices Order*).

[7] Greg Sandoval, *AT&T, Comcast May Help RIAA Foil Piracy*, CNET News (Jan. 28, 2009).

[8] *See infra* notes 38-42 and accompanying text; *see also* Patrick Foster, *Broadband Consumers to Foot £500m Bill to Tackle Online Piracy*, Times Online (Dec. 28, 2009); John Hopewell, *France's Anti-piracy Fight "Too Costly,"* Variety (Feb. 27, 2009).

[9] *See* Free Press, CHANGING MEDIA: PUBLIC INTEREST POLICIES FOR THE DIGITAL AGE 32 (2009) ("Nationwide, incumbent phone and cable companies control 97 percent of the fixed-line residential broadband market.").

own content and advertising over that of competitors. As the NPRM recognizes, switching costs and consumer lock-in may further undermine the ability of marketplace forces to prevent these practices.

Where market mechanisms cannot address these problems, there may be a place for narrowly tailored and carefully considered government regulation. Of course, government regulation carries its own drawbacks, often interfering with free speech and innovation even as it purports to protect them. The phenomenon of "regulatory capture," where an agency falls under the sway of the very industries it is supposed to be regulating, is another danger. The Commission's regulatory efforts are no exception to these risks.[10] These risks are compounded where the agency propounding regulations has no clear guidance from Congress, or where the scope of its regulatory authority lacks clear outer boundaries.

While the question of how to best protect the openness of the Internet is a timely and important one, it is not for the Commission to answer in the absence of statutory authority from Congress. Congress has not expressly delegated any authority to the Commission to issue the broad regulations on ISPs that it has proposed in the NPRM. Nor does "ancillary jurisdiction" provide an adequate jurisdictional basis. Accordingly, EFF believes that the Commission currently lacks the authority to issue enforceable regulations as contemplated by the NPRM.

If the Commission nevertheless chooses to forge ahead with the regulations proposed in the NPRM, EFF urges it to make revisions designed to protect the free speech and privacy interests of Internet users, and to foster competition and innovation.

---

[10] *See* Kurt Hunt, *The FCC Complaint Process And "Increasing Public Unease": Toward An Apolitical Broadcast Indecency Regime*, 14 MICH. TELECOMM. TECH. L. REV. 223, 238 (2007) ("the indecency complaint and investigation process seems incapable of removing itself from the political ebb and flow of politicians and interest groups, perhaps to the point of regulatory capture....").

First, in order to protect the free speech interests of Internet users, the Commission should reject copyright enforcement as "reasonable network management." Copyright enforcement has nothing to do with the technical business of network management. Moreover, the proposed regulations, by their terms, already exclude "unlawful content," making any exception for copyright enforcement unnecessary. Should ISPs want to deploy copyright enforcement technologies that inflict collateral damage on *lawful* content, those ISPs should be required to submit any such technologies to the Commission for pre-deployment review as part of a transparent public waiver process.

Second, in order to protect the privacy interests of Internet users, the Commission should clarify that the law enforcement exception applies only to an ISP's legal obligations to address the needs of law enforcement. Because the six proposed neutrality principles do not, by their terms, apply to unlawful content or activities, a general exception for law enforcement is unnecessary. Should ISPs want to voluntarily deploy technologies that would block *lawful* activity in the course of addressing the needs of law enforcement, those ISPs should be required to submit any such technologies to the Commission for pre-deployment review as part of a transparent, public waiver process.

Third, in order to protect the privacy interests of Internet users, the Commission should make it clear that its proposed regulations do not reach noncommercial providers of broadband Internet access service, whether they are individuals who operate open Wi-Fi networks at home, or public-minded entities that provide free Internet access in their local communities. The Commission should avoid the specter of federal regulation looming over noncommercial, public-spirited network providers. Federal regulation of these initiatives is not necessary to vindicate the openness, competition, innovation, and free expression goals of this proceeding.

Fourth, in order to foster competition and innovation, EFF urges the Commission to make it clear that the proposed "transparency" principle is not subject to an exception for "reasonable network management." As exemplified by the Commission's *Comcast Network Management Practices Order*, it is precisely when ISPs invoke the need for "reasonable network management" that the principle of transparency becomes most vital.[11] Only if ISPs are required to adequately disclose their network management practices will consumers, competitors, innovators, and the Commission be able to evaluate whether the practices are, in fact, "reasonable."

Fifth, in order to foster competition and innovation, the Commission should require wireless ISPs to allow "tethering" as a form of device interconnection. This requirement is a necessary corollary to the principle that consumers should be entitled to use any lawful device or application that does not harm the network. Tethering facilitates interoperability, competition, and openness. Furthermore, tethering blocks some troubling practices that are already emerging in the marketplace.

III. THE FCC LACKS THE STATUTORY AUTHORITY TO ADOPT THE PROPOSED RULES

"The FCC, like other federal agencies, literally has no power to act…unless and until Congress confers power on it."[12] The Commission cites no legislation that explicitly authorizes the regulations proposed in the NPRM.[13] Instead, the Commission relies on its "ancillary"

---

[11] *Comcast Network Management Practices Order*, *supra*, ¶¶ 52-53 (emphasizing harms that flow from Comcast's failure to adequately disclose its practice of blocking BitTorrent).

[12] *American Library Ass'n v. Federal Communications Comm'n*, 406 F.3d 689, 698 (D.C. Cir. 2005).

[13] NPRM ¶¶ 83-87. Although the Commission invokes its Title III authority with respect to wireless ISPs, this basis of authority obviously cannot sustain the regulations proposed by the NPRM to the extent they cover all broadband Internet access service providers.

jurisdiction, as it did in its *Comcast Network Management Practices Order*.[14] Ancillary jurisdiction, however, must be ancillary to some express grant of statutory authority.[15] Here, that necessary foundation is lacking. In other words, the proposed regulations "rest on no apparent statutory foundation and, thus, appear to be ancillary to nothing."[16]

The Supreme Court has made it clear that "the Commission was not delegated unrestrained authority" and does not have "unbounded" jurisdiction.[17] Yet the Commission's theory of ancillary jurisdiction as set forth in the NPRM effectively gives the agency plenary authority to regulate the Internet. In the words of Commissioner McDowell, "Under the analysis set forth in the [*Comcast Network Management Practices*] order, the Commission apparently can do *anything* so long as it frames its actions in terms of promoting the Internet or broadband deployment."[18] This unprecedented overreach raises the specter of discretionary FCC regulation of the Internet not just in the area of net neutrality, but also in a host of other areas.

Congress has not deputized the FCC to be a free roving regulator of the Internet. On the contrary, Congress has consistently preferred to *protect* the Internet from excessive regulation.[19] So while EFF strongly endorses the goals of this Commission as stated in the NPRM, a limitless notion of ancillary jurisdiction would stand as an open invitation to *future* Commissions to promulgate "policy statements," issue regulations, and conduct adjudications detrimental to the

---

[14] *Id.*

[15] *ALA v. F.C.C.*, 406 F.3d at 700 (exercise of ancillary jurisdiction requires that "the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities").

[16] *Id.* at 702.

[17] *Federal Communications Comm'n v. Midwest Video Corp.*, 440 U.S. 689, 706 (1979) (hereinafter *Midwest Video II*).

[18] Dissenting statement of Commissioner Robert M. McDowell, *Comcast Network Management Practices Order, supra*, at 63 (emphasis in original).

[19] *See* 47 U.S.C. § 230 (2008).

Internet. In EFF's view, the prospect of unelected Commissioners regulating the Internet without statutory constraint poses an intolerable risk to free speech, innovation, and competition.

EFF does not believe that the Commission has jurisdiction over ISPs sufficient to adopt and enforce the proposed regulations. The Commission and the courts agree that the Commission "may exercise ancillary jurisdiction only when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities."[20] The assertion of ancillary jurisdiction here fails to meet the second requirement.

Although the Commission invokes a number of statutory provisions[21] to support its exercise of ancillary jurisdiction here, none provide a sufficient statutory predicate for the proposed regulations. The Commission cites "federal Internet policy set forth by Congress in Section 230(b) of the Act, together with the broadband deployment goals that Section 706(a) charges the Commission with achieving."[22] Because these provisions, along with Section 1, are aspirational, hortatory statements of policy, they do not set forth "statutorily mandated responsibilities" to which the proposed regulations could be ancillary.[23] The Commission has

[20] NPRM ¶ 133.

[21] The NPRM incorporates by reference the jurisdictional discussion in the *Comcast Network Management Practices Order*, and presumably, the arguments the Commission has made before the D.C. Circuit Court of Appeals in defense of that *Order*. *See* NPRM ¶¶ 83-84; *Comcast Corp. v. Federal Communications Commission*, No. 08-1291 (D.C. Cir. brief filed Sept. 21, 2009).

[22] NPRM ¶ 84.

[23] *See* Barbara Esbin & Adam Marcus, *The Law is Whatever the Nobles Do: Undue Process at the FCC*, 17 COMMLAW CONSPECTUS 535, 563-610 (2009) (discussing in detail the unsuitability of Sections 1, 230(b) and 706 as bases for FCC ancillary jurisdiction).

recognized as much itself with respect to Section 706(a).[24] Moreover, Section 230(b)'s *deregulatory* purpose sets it *against* the regulations proposed by the NPRM, and the Supreme Court has made it clear that the Commission cannot rely on ancillary jurisdiction where the proposed regulations clash with the purposes of an express a statutory provision.[25]

Nor can Sections 201(b) or 257 provide a foundation for the proposed regulations. Section 201(b) provides the Commission with the procedural right to prescribe rules and regulations pursuant to statutory authority granted elsewhere. If Section 201(b) operated as a general authorization for the Commission to issue regulations whenever it concludes they might serve the "public interest," it would render the remainder of the Communications Act unnecessary.[26] Section 257, in contrast, is simply too meager a grant of authority—authorizing one rulemaking followed by triennial reports to Congress—to support the proposed regulations.[27]

The Supreme Court has made it clear that the Communications Act does not appoint the Commission as a roving regulator, with unbounded ancillary jurisdiction to regulate America's communications systems whenever, where ever, and however it likes.[28] The theory of ancillary jurisdiction espoused in the NPRM would accomplish just that, authorizing not only the

---

[24] *See In re* Deployment of Wireline Services Offering Advanced Telecommunications Capability, *Memorandum Opinion and Order and Notice of Proposed Rulemaking*, 13 F.C.C.R. 24,011, ¶ 69 (Aug. 6, 1998) ("[S]ection 706(a) does not constitute an independent grant of forbearance authority or of authority to employ other regulating methods.").

[25] *See* Esbin & Marcus, *supra*, at 587-596 (discussing the deregulatory purpose of Section 230); *Midwest Video II*, 440 U.S. at 700-07 (rejecting regulations that would have relegated cable broadcasters to common-carrier status despite contrary statutory purpose).

[26] *See id.* at 615-616 (discussing Section 201(b)).

[27] *Id*. at 618-620 (discussing Section 257); *Motion Picture Ass'n of Amer. v. Federal Communications Comm'n*, 309 F.3d 796, 807 (D.C. Cir. 2002) (noting that where statute authorizes the FCC only to issue a report, it cannot serve as authorization for broader regulations).

[28] *See Midwest Video II*, 440 U.S. at 706 (rejecting exercise of ancillary jurisdiction where it would leave FCC authority "unbounded").

proposed regulations, but also virtually any other measures that the Commission concludes would promote broadband deployment, "federal Internet policy," or the public interest generally. This outcome cannot be squared with good policy or with governing law. Accordingly, without further action by Congress, the Commission lacks the statutory authority to adopt the proposed regulations.[29] Nevertheless, EFF is hopeful that the factual record and recommendations developed in this rulemaking will provide valuable guidance to Congress as it develops legislation to address the issues addressed by the NPRM.

IV. COPYRIGHT ENFORCEMENT IS NOT REASONABLE NETWORK MANAGEMENT

The NPRM proposes that each of the six principles be made subject to the requirements of "reasonable network management."[30] The NPRM defines "reasonable network management" as "reasonable practices employed by a provider of broadband Internet access service to:

> (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns;
>
> (ii) address traffic that is unwanted by users or harmful;
>
> (iii) prevent the transfer of *unlawful content*; or
>
> (iv) prevent the *unlawful transfer* of content."[31]

[29] Congress has been considering several proposed "net neutrality" bills that would extend authority to the Commission to issue regulations regarding network management. *See, e.g.,* H.R. 3458 (2009); H.R. 5353 (2008). This also suggests that Congress itself does not believe the Commission has the authority to issue the proposed regulations without further statutory guidance. *See* Dissenting Statement of Commissioner Robert M. McDowell, *Comcast Network Management Practices Order*, *supra*, at 63 ("If Congress had wanted us to regulate Internet network management, it would have said so explicitly in the statute, thus obviating any perceived need to introduce legislation as has occurred during this Congress. In other words, if the FCC already possessed the authority to do this, why have bills been introduced giving us the authority we ostensibly already had?").

[30] NPRM ¶ 133.

EFF urges the Commission to delete the third and fourth elements of this definition. "Reasonable network management" includes practices that promote the proper *technical* functioning of an ISP's network. The Commission should not treat copyright enforcement or any other ISP efforts to block, interfere, or discriminate based on the content of speech—or based on the application or protocol a speaker chooses to express that speech—as "reasonable network management." Because the proposed regulations by their terms do not protect "unlawful content," there is no need for an exception to permit ISPs to block such content. Any copyright enforcement exception to the six principles simply serves to excuse ISPs from using undisclosed, overbroad techniques that interfere with *lawful* activities, as long as they claim they were attempting to restrict *unlawful* ones. This "copyright loophole" has profound implications for the free speech rights of Internet users and cannot be reconciled with the stated purposes of the NPRM.

The Commission should not adopt any exception that gives ISPs a green light to inflict "collateral damage" on lawful activities as a side effect of their efforts to block copyright infringement or unlawful conduct. ISPs are poorly placed to determine whether or not content is infringing or otherwise unlawful, a task generally reserved to attorneys, courts, and law enforcement. A loophole permitting overbroad mechanisms would give ISPs an incentive to be cavalier about making these difficult determinations. Second, the exception is not needed. ISPs—as well as content owners themselves (entities better placed to identify potential infringement)—already have a range of tools at their disposal to battle the problem without violating any of the six principles. Third, the exception could easily swallow the rule; ISPs could

[31] NPRM Appendix A, sec. 8.3 (emphasis added).

excuse any number of non-neutral practices by asserting that they were intended to target infringement.

In short, the issue that broadening the "reasonable network management" exception to include copyright enforcement and the blocking of unlawful content raises is not whether ISPs may undertake these efforts, but rather whether they may inflict collateral damage on *lawful* communications when they do so.

A. Any exception for reasonable network management should be limited to practices designed to ensure the proper technical functioning of the network

"Reasonable network management" is a term that is generally understood to mean practices that promote the proper technical functioning of an ISP's network, not efforts to determine whether any particular subscriber activity violates copyright law. The first two categories in the NPRM's proposed definition of the term reflect this commonsense understanding, addressing "reasonable practices employed by a provider of broadband Internet access service to (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; [or] (ii) address traffic that is unwanted by users or harmful."[32]

Allowing ISPs to block lawful content or activities in the name of copyright enforcement would undermine the basic goals of this proceeding. The Commission has stated that it seeks to vindicate the interests of consumers of Internet access services who may not be adequately protected by free market forces. An exception for "reasonable network management" is congruent with this goal, to the extent that the interests of consumers and ISPs may be aligned where genuine network management is at issue—better network management delivers a better product from the consumer's point of view. Steps taken to ensure faster speeds, less latency, more reliability, improved security, or fewer congestion delays are precisely the sorts of things

[32] *Id*.

that should qualify as "reasonable network management." In light of the alignment of incentives between ISPs and customers on these issues, the need for government intervention is likely to be less keen.[33]

Proposed network management practices that turn on the "legality" of the content or transmission are entirely distinct. These are areas where the interests of ISPs and consumers are not consistently aligned. For example, although ISPs have been under considerable public pressure to increase their efforts to address online copyright infringement, the pressure has not been from customers, but rather from the entertainment industry.[34] Network management in the interests of third parties is neither related to the technical functioning of the network, nor to meeting the demands of customers. Responding to these third party interests, ISPs may interfere with otherwise lawful customer activities for reasons unrelated to the provision of reliable or high quality Internet service. Customers whose lawful communications would suffer as a result of ISP acquiescence to third party pressure may have difficulty finding an alternate broadband Internet access provider. Accordingly, the six principles should intervene to protect the interests of those whose *lawful* activities might get swept up in overbroad efforts to block or discriminate against infringing or otherwise unlawful content.

B. The proposed regulations do not prohibit blocking unlawful content, and thus there is no need for an exception for copyright enforcement

The structure of the proposed regulations already allows copyright enforcement and other efforts to block "unlawful content or traffic." As drafted, the six principles exclude unlawful content from their scope. For example, according to the proposed sixth "nondiscrimination"

---

[33] As noted below, EFF does not believe that the principle of transparency should give way to "reasonable network management."

[34] Marguerite Reardon, *Should AT&T Police the Internet*, CNET News (Jan. 17, 2008); Anne Broache, *MPAA Wants ISP Help on Online Piracy Fight*, CNET News (Sept. 18, 2007).

principle, an ISP "must treat *lawful* content, applications, and services in a nondiscriminatory manner."[35] The first, second, and third principles include similar language limiting their scope.[36] The NPRM confirms that the principles are not meant to protect unlawful content or activities.[37]

Accordingly, there is no need for any exception (whether under "reasonable network management" or otherwise) to allow ISPs to block unlawful content or unlawful transfers of content. The six principles are only implicated when an ISP employs practices, whether in the name of copyright enforcement or otherwise, that interfere with a consumer accessing *lawful* content, using *lawful* devices, running *lawful* applications, or accessing *lawful* services.

In other words, *copyright enforcement efforts will only run afoul of the six principles to the extent they inflict collateral damage on lawful content and activities*. Viewed in this light, there is no basis for granting a general exception in the name of copyright enforcement. It is precisely the business of the six principles to *prevent* ISPs from engaging in practices that improperly sacrifice *lawful* content or activities in the name of blocking copyright infringement or other unlawful content.

C. This exception will cause serious collateral damage

1. Overbroad copyright enforcement mechanisms put lawful content and activities at risk

The risks posed to innocent users by overbroad measures aimed at curtailing copyright infringement are far from hypothetical.[38] A group of researchers at the University of

---

[35] NPRM Appendix A, § 8.13 (emphasis added).

[36] *Id.* at §§ 8.5, 8.9, 8.11.

[37] NPRM ¶¶ 96-97.

[38] *See, e.g.*, Mehan Jayasuria et al., *Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs*, at 43-44 (noting an additional 100 ms of delay translated into a 1 percent drop in sales for Amazon.com, and that a 500ms delay resulted in a 20 percent drop in traffic for Google).

Washington, for example, reported that weaknesses in online copyright enforcement techniques resulted in the university receiving numerous infringement allegations for IP addresses that were exclusively used by laser printers unable to share any copyrighted files. The researchers concluded that "[t]he potential for false positives and implication of arbitrary [IP] addresses undermines the credibility of monitoring and creates a significant inconvenience for misidentified users (if not financial and/or legal penalties)."[39]

A computer science researcher at Princeton University similarly found that dozens of infringement notices erroneously identified a research system he operated as a source for BitTorrent sharing, despite the fact that no BitTorrent clients were running on the system. "Thus, we can fairly definitively conclude that the [enforcement agent who sent the notices] never actually tested the peer for actual infringement: not even by trying to connect to the client's address, let alone determining whether the client was actually uploading or download[ing] any data, and let alone valid data corresponding to the copyrighted file in question."[40]

YouTube's automated "Content I.D." system, currently among the most advanced systems to identify copyrighted works, has frequently been used in ways that have censored noninfringing materials. For a period of several months in 2009, for example, the Warner Music Group (WMG) set YouTube 's "Content I.D." filter to remove all videos identified as containing any WMG music. As a result, twice as many videos were removed from YouTube in January 2009 as in the *entire previous year combined*. The deleted videos included clear fair uses like a

[39] Michael Piatek, Tadayoshi Kohno & Arvind Krishnamurthy, Challenges and Directions for Monitoring P2P File Sharing Networks, or, Why My Printer Received a DMCA Takedown Notice (2008).

[40] Mike Freedman, *Inaccurate Copyright Enforcement: Questionable "Best" Practices and BitTorrent Specification Flaws*, Freedom to Tinker blog (Nov. 23, 2009).

homemade instructional video by a sign language teacher and a video that parents recorded of their four-year-old lip-synching.[41]

As difficult as *identifying* a copyrighted work is, making a determination about its *legality* is even harder. For example, in its high-profile lawsuit against YouTube, Viacom recently had to withdraw infringement allegations regarding 250 works after an apparently belated realization that those works were, in fact, authorized to be on YouTube or otherwise not infringing.[42] If Viacom's own lawyers make mistakes regarding the legal status of its own works, it is a certainty that ISPs will make mistakes that will imperil lawful content unless that content enjoys the protections of the six principles.

2. An exception for copyright enforcement could threaten to swallow the six principles

A broad copyright enforcement exception endangers the six principles by giving ISPs a pretext behind which to hide otherwise forbidden practices. ISPs could target particular applications, protocols, or services for discriminatory treatment, all the while asserting that they were merely targeting copyright infringement. In fact, a broad copyright enforcement exception to the six principles could give ISPs and copyright owners an incentive to collude to evade the six principles, with copyright owners providing ISPs with "cover" before the Commission for anticompetitive ISP practices.

Consider the Commission's 2008 *Comcast Network Management Practices Order*. Plainly, Comcast should not have been able to prevail in that adjudication simply by "changing its story" and arguing that its clandestine BitTorrent blocking was intended to curtail copyright

[41] Corynne McSherry, Careless Copyright Owners, Automated Takedowns: A Disaster for Online Creativity, ACSblog (Mar. 28, 2009).

[42] Wendy Davis, *Google Lawyer Claims Viacom Request Undermines Its Charge Of Copyright Infringement*, Media Post Online Media Daily (Dec. 29, 2009).

infringement. Yet future ISPs could achieve this perverse result if copyright enforcement mechanisms were exempted from the six principles as "reasonable network management," as proposed in the NPRM.

To the extent that ISP practices purportedly aimed at curtailing copyright infringement or other unlawful activities also interfere with lawful content and activities, they pose the same dangers to competition, innovation, and openness that other practices that violate the six principles would. For example, if ISPs deploy undisclosed mechanisms in the name of copyright enforcement that selectively block protocols or applications, innovators who want to offer new products and services may have to negotiate with ISPs, hat in hand, to ensure that their products will not be thwarted by these mechanisms. Accordingly, the Commission should make it clear that all lawful content is protected by the six principles, notwithstanding efforts by ISPs to justify inflicting collateral damage on lawful activity in the name of blocking infringing or otherwise unlawful content.

3. There are many existing alternatives for addressing copyright infringement and unlawful content that do not violate the six principles

There are many mechanisms that ISPs can employ to curtail unlawful activity, including copyright infringement, that do not run afoul of the six principles. Content owners themselves (who are better placed to determine infringement than ISPs, although not as well-suited as courts) already have a range of tools at their disposal to battle copyright infringement. For example, copyright infringement is subject to stiff civil remedies as well as criminal penalties. The Digital Millennium Copyright Act (DMCA), moreover, has given ISPs strong incentives to respond expeditiously to "takedown notices," providing copyright owners a powerful tool to

remove infringing material from the Internet without having to resort to the courts.[43] Many ISPs have also agreed to forward infringement notices to subscribers—another mechanism that falls outside the scope of the six principles. Further, nothing in the six principles would prevent ISPs from choosing not to do business with subscribers who are engaged in illegal activities. In summary, there is no evidence that lawful content or activities must be sacrificed in order to make headway against copyright infringement.

D. Copyright enforcement practices that would inflict collateral damage on lawful activities should be subject to a pre-deployment public review process

For the reasons explained above, the Commission's proposed definition of "reasonable network management" should be revised to eliminate the provisions addressing "the transfer of unlawful content" and "unlawful transfer of content." This revision would not shield unlawful content or activities—as discussed above, ISPs remain unconstrained by the six principles so long as their practices do not affect lawful content.

If an ISP wants to adopt practices that would violate the six principles with respect to *lawful* content or activity in the course of curtailing unlawful content on its network, it should be required to apply for a waiver from the Commission prior to deployment of such practices. In the interests of promoting transparency, the waiver proceeding should be subject to public comment and review. The ISP should be required to meet a high threshold before being allowed to deploy overbroad measures that disadvantage or discriminate against lawful content. That is, the

[43] At the same time, content owners who use these legal mechanisms can be held accountable when they do so improperly. 17 U.S.C. §512(f); *Fogerty v. Fantasy*, 510 U.S. 517 (1994). Thus innocent infringers and customers whose use of material is protected by fair use, first sale or other doctrines have some recourse when they are falsely accused. By contrast, a customer whose Internet communication is blocked or degraded has only two options, if she learns about the interdiction at all. She may try to find another provider (assuming alternatives exist in her local market) or figure out how to "bypass" the ISP's interdiction efforts though encryption or some other mechanism.

Commission should require providers to submit a proposed strategy/technology for review and comment in advance, so that FCC, the service provider's customers, and companies seeking to develop new products and services can consider whether the proposed mechanism will unfairly restrict their ability to engage in fair uses or other legal activity and/or offer new products and services.

Waivers should be conditioned on an ISP demonstrating that the practice meets the requisite standard, depending on the context and practice used, with careful attention to possible impacts on free speech. As part of this inquiry, the Commission should evaluate, at a minimum: (1) whether and how the impact to lawful content has been minimized; (2) whether alternatives that restrict less speech are available; (3) the likelihood that the practice will be effective at curtailing unlawful activity; and (4) whether the effort to curtail unlawful content creates too great a risk of impeding legitimate innovation, competition or speech interests. Any waivers granted should be for limited times, subject to regular re-evaluation in light of changing technologies.

V. ANY LAW ENFORCEMENT EXCEPTION SHOULD BE LIMITED TO LEGAL OBLIGATIONS

As explained above, the six principles proposed by the NPRM by their terms exclude unlawful content and activity from their scope. This makes a broad exception for practices undertaken by ISPs to address the needs of law enforcement unnecessary. EFF thus urges the Commission to draw the law enforcement exception to the six principles narrowly to reach only an ISP's legal obligations with regard to the enforcement of federal criminal law. If ISPs at some point wish to adopt practices to address the needs of law enforcement that would inflict collateral damage on *lawful* content or activities in violation of the six principles, the Commission should

permit those practices only after they are first submitted to the Commission for a searching pre-deployment review as part of a public waiver process.

The NPRM includes an exemption to the six principles where ISPs adopt practices in order to address the needs of law enforcement:

> *Nothing in this part supersedes any obligation a provider of broadband Internet access service may have—or limits its ability—to address the needs of law enforcement, consistent with applicable law.*[44]

The proposed phrasing of the law enforcement exception suggests that providers may violate FCC's network neutrality rules either to fulfill their legal obligations or to voluntarily address the needs of law enforcement, subject to other applicable laws.

EFF urges the Commission to revise its proposal to clarify that ISPs may transgress the six principles (i.e., inflict collateral damage on *lawful* content and activities) to fulfill their legal obligations, but may not use law enforcement needs as an excuse to *voluntarily choose* to violate the principles with respect to lawful activities. Accordingly, EFF proposes the following revised formulation:

> *Nothing in this part limits the ability of a provider of broadband Internet access service to meet its legal obligations to address the needs of law enforcement, consistent with applicable law.*

As explained above, the proposed regulations by their terms already exclude unlawful content and activities. Accordingly, there is nothing in the six principles that would constrain an ISP's ability to address the needs of law enforcement, so long as only unlawful content or activity is affected. Put another way, any exception to the six principles for practices undertaken in the name of law enforcement would be an exception that permits discrimination against *innocent, lawful* conduct.

---

[44] NPRM ¶ 143.

Moreover, the proposed regulations would not interfere with voluntary efforts by ISPs that do not transgress the six principles. So, for example, information gathering, retention, or disclosure that does not involve discriminating among, or blocking access to, content, applications, or services would not violate the regulations, and so no exemption would be needed.[45]

Finally, this exception would not interfere with the ability of federal criminal law enforcement authorities to *obligate* ISPs to help them enforce criminal law through existing statutory means. CALEA[46] requires ISPs to ensure they have built-in surveillance capabilities so federal agencies can monitor broadband Internet and VoIP traffic in real-time. State and federal authorities may compel both real-time surveillance and access to stored content and transactional records through the Electronic Communications Privacy Act[47] and the Pen Register/Trap and Trace Statute.[48] Even civil parties have access to some kinds of ISP records through third party subpoenas and the normal civil discovery process.[49]

In short, ISPs need no exception to the six principles in order to assist law enforcement in targeting unlawful content or activities. They also need no exception to the six principles to the extent their voluntary efforts to address law enforcement needs do not transgress the six principles (i.e., do not inflict collateral damage on innocent, lawful activities). In addition, the reformulated exception proposed here makes it clear that ISPs may cooperate with law enforcement pursuant to a legal obligation, even where such cooperation would interfere with

[45] Of course, such activities may violate other applicable laws, but the proposed regulations make it clear that nothing therein relieves an ISP of its obligation to comply with all other laws.

[46] Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (1998).

[47] 18 U.S.C. §§2510 et seq.

[48] 18 U.S.C. § 3121.

[49] *See, e.g., Doe v. 2TheMart.com*, 140 F.Supp.2d 1088 (W.D. Wash. 2001).

lawful conduct in a manner that violates the six principles. Federal law enforcement authorities have and will continue to have a wide array of tools that obligate ISPs to help them enforce criminal law.

Not only is a broad exception for voluntary efforts undertaken on behalf of law enforcement unnecessary, but if adopted could threaten to swallow the six principles. ISPs would be able to cloak discriminatory practices with an assertion that such practices were intended to assist law enforcement. In fact, such a scenario could yield perverse results, as ISPs might develop non-neutral practices for anticompetitive reasons, then seek the imprimatur of law enforcement agencies in order to evade the six principles.

If an ISP at some point wants to adopt practices that would violate the six principles with respect to otherwise lawful content or activity in order to address the needs of law enforcement, it should be required to apply for a waiver from the Commission prior to deployment of such practices. In the interests of promoting transparency, the waiver proceeding should be subject to public comment and review. The ISP should be required to meet a high threshold before being allowed to deploy overbroad measures that disadvantage or discriminate against lawful content. That is, the FCC should require providers to submit a proposed strategy/technology for review and comment prior to deployment, so that the Commission, the service provider's customers, and companies seeking to develop new products and services can consider whether the proposed mechanism will unfairly restrict their ability engage in legal activities and/or offer new products and services.

Waivers should be conditioned on an ISP demonstrating that the practice meets the requisite standard, depending on the context and practice used, with careful attention to possible impacts on free speech. As part of this inquiry, the Commission should evaluate, at a minimum:

(1) whether and how the impact to lawful content has been minimized; (2) whether alternatives that restrict less speech are available; (3) the likelihood that the practice will be effective at curtailing unlawful activity; and (4) whether the practice in question creates too great a risk of impeding legitimate innovation, competition or speech interests. Any waivers granted should be for a limited time, subject to regular re-evaluation in light of changing technologies.

VI. THE TRANSPARENCY PRINCIPLE SHOULD NOT BE SUBJECT TO REASONABLE NETWORK MANAGEMENT

If the Commission decides to adopt the proposed regulations contained in the NPRM, EFF strongly endorses the sixth principle, aimed at guaranteeing transparency with respect to relevant network management practices. In order to foster competition and innovation, however, EFF urges the Commission to make it clear that the proposed transparency principle (1) is not subject to an exception for "reasonable network management" and (2) applies to ISP practices undertaken pursuant to the law enforcement, public safety, and homeland and national security exceptions.

The NPRM formulates the transparency principle as:

> *Subject to reasonable network management, a provider of broadband Internet access service must disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections specified in this part.*[50]

EFF urges the Commission to revise the proposal as follows:

> *A provider of broadband Internet access service must disclose such information concerning network management and other practices (including practices undertaken to address the needs of law enforcement, public safety or national security or homeland security authorities) as is reasonably required for users and content, application, and service providers to enjoy the protections specified in this part.*

[50] NPRM ¶119.

Transparency is critically important. Competitors, customers, and innovators must have adequate information regarding network management practices. Without adequate information, customers will not be able to express their preferences by switching ISPs, which, in turn, would interfere with and distort market mechanisms that protect consumers and correct improper ISP practices. A further risk is that the customer may punish the wrong party, by blaming the application vendor, device maker, or herself for the problem.

In addition, competing ISPs need full information in order to develop and market alternative broadband service to customers. Full information encourages competing ISPs to improve and innovate on their broadband networks, confident that such improvements will yield a marketplace edge over competitors. Without transparency, customers cannot effectively and efficiently reward these innovative ISPs in the marketplace for their efforts.

Critically, innovators must also be given enough information to enable them to develop new applications and protocols that work reliably without asking permission from ISPs. In the absence of transparency regarding network practices that implicate the proposed principles, constant uncertainty regarding network behavior will operate as a serious barrier to new Internet technology developers. The cost of investigating the unexpected behavior of a piece of software sufficiently to diagnose a problem caused by malfunctioning or misconfigured network management systems should not be underestimated. In many instances, such costs may be greater than small innovators can afford.

In light of the importance of transparency, an ISP's transparency obligation should not be excused for "reasonable network management." For all the reasons noted above, whether or not an ISP's network management practices are "reasonable," if they interfere with any of the protections afforded by the first five principles, they should be disclosed to consumers,

competitors, and innovators. In other words, even if violations of the first five principles can be excused in the interests of "reasonable network management," that is no justification for allowing an ISP to maintain those practices in a climate of secrecy.

The Commission's *Comcast Network Management Practices Order* underscores the importance of transparency, especially in the face of an ISP's assertion of "reasonable network management."[51] Only after Comcast was required by the Commission to describe its network management practices in detail were consumers, competitors, and public interest groups (and ultimately the Commission) able to evaluate the validity of Comcast's justification.

For the same reasons, the Commission should make it clear that the transparency principle applies where an ISP implements practices to address the needs of law enforcement, public safety, national security, or homeland security authorities that would otherwise implicate any of the first five principles. The need for transparency in these circumstances is essential to the Commission's proposed case-by-case adjudicatory approach to enforcing the proposed regulations. If ISPs were free to implement these practices without disclosure, those whose lawful content and activities were affected would find it difficult—if not impossible—to challenge those practices before the Commission.

VII. NON-COMMERCIAL PROVIDERS OF BROADBAND INTERNET ACCESS SERVICE SHOULD BE EXEMPTED FROM THESE RULES

The Commission has defined "broadband Internet access service" to exclude "establishments that acquire broadband Internet access service from a facilities-based provider to enable *their patrons or customers* to access the Internet from their respective establishments," such as coffee shops, waiting rooms, or rest areas.[52] The Commission similarly proposes to

[51] *Comcast Network Management Practices Order*, *supra*, at ¶¶ 52-53.

[52] NPRM ¶ 55 (emphasis added).

exclude "broadband Internet access service that is *not intentionally offered for the benefit of others*, such as service from personal Wi-Fi networks whose signal may be detectable outside the user's premises."[53] While we applaud the Commission's effort to minimize the regulatory burden on these entities, EFF believes the Commission should revise the definition to exclude all noncommercial providers of broadband Internet access service.

First, this revised exclusion should cover all personal Wi-Fi networks, whether or not they are "intentionally offered for the benefit of others." Millions of Americans have Wi-Fi access points connected to their cable modems or DSL lines. Many choose to leave their access points "open" in order to allow neighbors and passersby to connect to the Internet. Both ISPs and hardware manufacturers cater to these individuals. National DSL provider Speakeasy, for example, has a "wireless sharing policy" that encourages subscribers to share their broadband connection with neighbors.[54] Similarly, Apple's Airport Extreme Wi-Fi access point offers a "guest networking" feature, billed by Apple as making it "easy to allow guests to use your Internet connection without sharing your password or giving them access to the rest of your network."[55]

The Commission should not impose regulatory burdens on individuals who use these products and services to offer Internet access to their neighbors. After all, if a Good Samaritan chooses to offer free Internet access to her neighbors, there is no harm if she chooses to engage in behavior that violates the six principles. For example, she should be free to block iPhones from joining her network if she dislikes Apple, or to ban YouTube if she disapproves of Google. While these actions, if undertaken by a major facilities-based ISP, could have the negative

---

[53] *Id*. (emphasis added).

[54] *See* Speakeasy website, Wireless Sharing Policy.

[55] *See* Apple website, Airport Extreme—Features description.

effects described by the Commission in the NPRM, Wi-Fi networks shared by individuals do not pose the same risks.

Second, the exclusion should reach beyond establishments that offer Wi-Fi access solely to their "patrons or customers." While coffee shops, airports, libraries, and hotels often provide complementary wireless access to patrons and customers, there are other publicly minded entities that offer Wi-Fi more broadly as a community service. Many public libraries, for example, offer wireless Internet access that intentionally reaches adjoining public places. A coalition of merchants and organizations offers free Wi-Fi access in Harvard Square.[56] A project known as "Free the Net" has organized volunteers to deploy free public Wi-Fi in many parts of San Francisco.[57] The not-for-profit Public Internet Project brings free wireless Internet access to Bryant Park in New York City.[58] There are myriad similar efforts underway throughout the United States.

While the prospect of the Commission being called upon to enforce the six principles against these small, public-spirited wireless networks may seem far-fetched, the Commission should nevertheless avoid leaving the specter of federal regulation looming over them. Federal regulation of these small, public-minded initiatives is not necessary to vindicate the goals of this proceeding (openness, competition, innovation, free expression). These network operators may want to block certain applications or protocols in order to favor web browsing over other applications, to minimize community complaints, or for other arbitrary reasons[59] (wise or

---

[56] *See* Nick Barber, *Businesses, City Launch Free Public Wi-Fi in Harvard Square*, PC World (June 5, 2008).

[57] *See* Meraki, Free the Net San Francisco.

[58] *See* Public Internet Project.

[59] For example, one person prankishly modified his personal open wireless network to display web pages upside down, *see* Upside-Down-Ternet.

unwise, intentional or unintentional). If they are required to research and comply with FCC regulations, or to report in detail to potential users what their network practices are, the burden of compliance may simply convince them to give up the effort, to the detriment of competition and broadband deployment.

Moreover, users generally have choices other than noncommercial community providers. The user can go to a different coffee shop or hotel, sign up for Internet access at home, or connect to the Internet in other ways. The FCC should not impose regulations that would unduly burden and thereby interfere with the proliferation of noncommercial Wi-Fi connection points.

VIII. WIRELESS PROVIDERS SHOULD BE REQUIRED TO ALLOW TETHERING

In the NPRM, the Commission asks whether, in the wireless Internet context, it should "require providers to allow 'tethering' as a form of device interconnection?"[60] EFF believes that the Commission should do so. Allowing consumers to use their Internet-capable handsets as modems to connect with other devices is a necessary corollary of the proposed third principle of device and application neutrality as applied to wireless carriers. It also represents the simplest method of bringing the principles first announced in the landmark 1968 *Carterfone* ruling to bear in the wireless context.[61]

The Commission correctly notes that "[t]ethering is not universally permitted by providers."[62] In fact, the lack of tethering has become a recurring complaint among a growing number of customers, particularly those who use advanced broadband-capable handsets such as

---

[60] NPRM ¶ 167.

[61] *See generally* Tim Wu, Wireless Net Neutrality: Cellular *Carterfone* and Consumer Choice in Mobile Broadband, New Am. Working Paper No. 17 (2007) (explaining the need to embrace in the wireless context the device neutrality principles announced in the 1968 *Carterfone* ruling).

[62] NPRM ¶ 164.

the Apple iPhone and Motorola Droid.[63] The widespread availability of tethering in countries other than the United States makes it clear that these services are technically and commercially feasible.[64]

Moreover, given that tethering capabilities are already a standard feature among broadband-capable handsets, tethering represents a practical, extant, and deployed "standard network interface" that permits a broad array of devices and applications to connect to the wireless Internet. The development of standard network interfaces is crucial to the *Carterfone* principle—the deployment of the RJ-11 phone jack, for example, accelerated the development of the myriad devices that were able to interconnect to the landline telephone network.[65] And while there are already standardized "air interfaces" for cellular networks—built on the GSM and CDMA standards—cellular handsets offering Bluetooth or Wi-Fi interfaces for tethering (as the iPhone does) will immediately open up the wireless Internet to a much wider array of devices and applications already in the market.

Wireless carriers are likely to argue that the bandwidth constraints of their networks make tethering impractical. This argument does not withstand scrutiny. Many wireless carriers already tolerate a wide array of third party applications on smartphones without any mechanism to block applications that might be "bandwidth hogs." There is no reason to assume that users who want to employ tethering will use more bandwidth than those using high-bandwidth

---

[63] *See* Prince McLean, *AT&T fails to deploy iPhone Tethering and 3G MicroCell in 2009*, Apple Insider, Dec. 31, 2009; Tim Stevens, *Verizon confirms DROID tethering cost, will ask subscribers to double-down on their data plan*, Engadget, Nov. 6, 2009.

[64] *See id*.

[65] Tim Wu, *Wireless Carterfone*, 1 INT'L J. OF COMM. 389 (2007). *See also* Skype Communications S.A.R.L, Petition to Confirm a Consumer's Right to Use Internet Communications Software and Attach Devices to Wireless Networks, RM-11361, at 9 (filed Feb. 20, 2007).

applications on the phone itself. For example, Apple has publicly stated that AT&T has no say over the App Store approval process for iPhone applications.[66] And bandwidth-intensive applications—such as Showtime, DirecTV's NFL Superfan, MLB.com At Bat, and TVUPlayer—are available from the App Store.[67] If iPhone users are able to use approved apps to consumer large amounts of bandwidth, it does not make sense to penalize those who want to use tethering for low-bandwidth activities like downloading email to a laptop while traveling.

If carriers are concerned about managing bandwidth scarcity and preventing congestion, there are more narrowly tailored ways to address this concern, such as employing protocol- and application-neutral traffic shaping systems or charging those who exceed a prescribed bandwidth cap, rather than arbitrarily blocking tethering while permitting other bandwidth-intensive applications on the phone itself. In short, the problem is not tethering, or the devices and applications that can attach through a tethering interface, but rather what the customer does with the attached device or application (whether on the phone itself or a laptop connected through the phone). While carriers should be permitted to engage in reasonable network management (subject to the transparency principle), the Commission should not permit "reasonable network management" to be used as a pretext for trampling the user's freedom to connect the device of her choice to the network or use the application of her choice on that device.

IX. CONCLUSION

Customer choice is the first line of defense against ISP filtering and blocking of lawful communications, protocols, applications and devices. But since few Internet users have meaningful choices among residential broadband providers, and since business incentives and

[66] Apple.com, Apple Answers the FCC's Questions (stating that Apple alone makes the decision whether to approve an iPhone application).

[67] *See* MLB at Bat for iPhone; DirecTV NFL Superfan; TVU Player; Showtime Mobile.

third party pressure may increasingly place ISPs at odds with their customers, there may be a place for narrowly tailored and carefully considered government regulation. However, the FCC does not currently have the authority to issue such regulations in the absence of clear guidance from Congress and clear outer boundaries for its regulatory authority. Should the FCC decide nevertheless to issue regulations in the name of network neutrality, the regulations should not contain a copyright loophole nor carelessly allow voluntary discrimination under the guise of aiding law enforcement. The rules should also encourage the development of customer choice and market options by ensuring tethering, promoting noncommercial Wi-Fi, and ensuring that consumers and innovators have the information they need about the network management practices of ISPs.

DATED: January 14, 2010

By _____*Fred von Lohmann*_____

Fred von Lohmann
Senior Staff Attorney
fred@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x123
Facsimile: (415) 436-9993