

A cross-platform indirect network effect is a type of indirect network effect that occurs through the compatibility of different platforms. Imagine a Web-based sports information service application, which becomes popular. If the same non-discrimination rules that apply in the broadband Internet wireline access space apply to the broadband Internet wireless access space, then the application provider has the incentive to improve its product offerings, including the functionality available to wireless users. The new product creates new value for the wireless network, as well as to users of the wireless network. Thus, there is an indirect network effect that creates a positive spillover for wireless network users even though the application was originally created for wireline broadband networks.⁵⁹

VII. DEFINING THE SCOPE OF “REASONABLE NETWORK MANAGEMENT”

In assessing what is “Reasonable Network Management,” the Open Internet Coalition urges the Commission to develop a two-step framework that answers two basic questions;

- First, does the network management practice further a legitimate purpose?
- Second, is the means narrowly tailored to address that purpose?

The OIC agrees with the FCC that there is a strong interest in reducing or mitigating the adverse affects of network congestion that supports reasonable

⁵⁹ See Hogendorn at 8.

network management practices. Generally, there are two categories of network management practices – (a) technical traffic management practices and (b) economic traffic management practices.⁶⁰

A. Increasing Capacity Has Been the Best Approach to Addressing Issues Relating to Congestion

Before discussing whether specific techniques to address congestion are reasonable, it is important to note that the best solution for congestion problems – which have been consistently effective as the Internet has grown – is investing in faster, better networks. Leading technologists have recognized this fact.⁶¹ In October 2009, the Canadian Radio-television and Telecommunications Commission made such a finding in its “Review of the Internet traffic

⁶⁰ Technical traffic management practices include slowing down a user’s traffic, prioritizing traffic, and limiting the bandwidth of large bandwidth users. Economic traffic management practices include monthly bandwidth capacity limits, where users who exceed a predefined threshold must pay additional money for bandwidth consumed and time-of-day pricing for bandwidth consumed. See Telecom Regulatory Policy CRTC 2009-657, Paragraph 20.

⁶¹ The non-profit networking consortium Internet2 found increasing capacity to be the most economically and technologically efficient solution for congestion. Internet2 is a not-for-profit advanced networking consortium comprising more than 200 U.S. universities in cooperation with 70 leading corporations, 45 government agencies, laboratories, and other institutions of higher learning as well as over 50 international partner organizations. See <http://www.internet2.edu/about>; See also Steven Corbato and Ben Teitelbaum, “Internet2 and Quality of Service: Research, Experience, and Conclusions,” pg. 4, May 2006.

management practices of Internet service providers.”⁶² In May 2008, leading Japanese telecommunications, cable, and Internet providers groups reached the same conclusion.⁶³ Next generation broadband networks not only solve problems of congestion, but they promote innovation by encouraging the development of more robust applications and content from which both consumers and the economy benefit.

The most technologically and economically efficient means of managing Internet traffic is by increasing capacity. The advanced networking consortium Internet2 confirmed this proposition when it contrasted the introduction of Quality of Service (“QoS”) electronics with increasing capacity as a means of addressing congestion.⁶⁴ QoS electronics are the hardware that make the manipulation of Internet traffic possible.

⁶² “Network investment is a fundamental tool for dealing with network congestion and should continue to be the primary solution ISPs use,” Telecom Regulatory Policy CRTC 2009-657, October 21, 2009, P.1.

⁶³ “In the first place, ISPs, etc. should tackle the increase in traffic by enhancing its network capacity,” Guideline for Packet Shaping, Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Services Association, Japan Cable and Telecommunications Association, May 2008.

⁶⁴ Beginning in 1998 through 2001, technical leaders from Internet2 worked to develop and deploy an advanced Internet Protocol serviced based on Quality of Service (QoS) technology. This project launched when a large portion of the Internet2 technical community initially believed that implementing QoS would be essential to addressing network congestion due to increasing demand for limited bandwidth, especially applications such as streaming video or videoconferencing, which applications do not tolerate packet loss or jitter.

Internet2 found that increasing bandwidth is far superior to adding QoS electronics:

[Increased bandwidth] avoided practical deployment obstacles to implementing any effective QoS across a multiple network environment such as the Internet. Specific obstacles include: coordinating upgrades to QoS technology across every network; changing dramatically network operations, peering arrangements, and business models; and developing suitable means to verify QoS service delivery by users, providers, or both.⁶⁵

Internet2 found that the “over provisioning” of bandwidth approach to ensure network performance has been made possible by new technology that provided geometric increases in networking capacity at rates that matched or exceeded Moore’s Law.⁶⁶

Internet2’s experience led it to conclude that increasing capacity is the most economically and technologically efficient means of addressing congestion:

Instead of implementing QoS, simply increasing network speed leverages the decreasing cost-per-bit trend of new networking technologies and avoids the pitfalls of QoS implementation. The elegant simplicity of the best-effort service model provided by IP is one of the essential reasons for the success of the Internet. Together

⁶⁵ Corbato and Teitelbaum, “Internet2 and Quality of Service: Research, Experience, and Conclusions,” May 2006, p.2. See also, Bhagat, Smriti “QoS: Solution Waiting for a Problem”. Professor Bhatat’s paper concludes that over provisioning of bandwidth is preferable to QoS technology in addressing network congestion. Available at: <http://www.cs.rutgers.edu/~rmartin/teaching/spring06/cs553/papers/004.pdf>

⁶⁶ Moore’s Law refers to the observation in 1965 by Gordon E. Moore, co-founder of Intel that the complexity of integrated circuits doubles every 24 months with improvements in manufacturing methods.

with the inherent strengths of connectionless networking and the IP's end-to-end design principle, the best-effort service model has enabled a fast, dumb, cheap, and wildly scalable Internet which has, in turn, provided a foundation for manifold innovative uses, unconstrained by a centralized view of how the network can or should be used.⁶⁷

Indeed, though broadband Internet access providers do not currently make transparent data relating to growth of traffic on their networks, recently Cisco predicted that between 2007-2012, Internet traffic will increase 46 percent a year, nearly doubling every two years.⁶⁸ This prediction is consistent with data provided by TELUS, a Canadian ISP, which showed that Internet traffic essentially doubled from January 2006 to January 2008.⁶⁹ Applying Moore's Law, Internet2's study demonstrates that broadband Internet access providers should be able to handle growth in Internet traffic without the introduction of QoS electronics as bandwidth capacities will be able to at least correspondingly double over the same period of time.

Adding capacity is an important public policy goal though the OIC is not suggesting that the Commission regulate broadband Internet access providers to

⁶⁷ Corbato and Teitelbaum, p. 4.

⁶⁸ "Cisco Visual Networking Index Projects Global IP Traffic to Reach Over Half a Zettabyte(1) in Next Four Years," Press Release, June 16, 2008, available at http://newsroom.cisco.com/dlls/2008/prod_061608b.html.

⁶⁹ TELUS (CRTC) 4Dec08-1. The TELUS data indicates that the total amount of Internet traffic into and out of the TELUS core backbone network essentially doubled from January 2006 to January 2008. The total megabits per second increased during this time period from 32,390 to 70,651.

require increased network capacity. Rather, the Commission should adopt rules in this proceeding that encourage additional private investment in increased capacity.

Allowing discrimination would have the exact opposite impact. It would create a perverse incentive for broadband Internet access providers to maintain scarcity, rather than expand capacity. If, for example, broadband providers can make money by charging content and application providers for prioritization in a special “fast lane,” they will have a new incentive to keep the “slow lane” slow. Such a perverse incentive would be at odds with the goals of the Communications Act.⁷⁰

One way to eliminate such an incentive is to remove from a broadband Internet access provider the inappropriate crutch of network management practices that are not narrowly tailored. A narrowly tailored network management practice is one that is designed to address a defined, temporal need and nothing more.⁷¹

⁷⁰ See 47 U.S.C. § 254(b)(2) (“Access to advanced telecommunications and information services should be provided in all regions of the Nation.”); Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 153 (1996), *codified as amended at* 47 U.S.C. § 1302; 47 U.S.C. § 230; *see also* 47 U.S.C. § 1305(k)(2) (“The national broadband plan required by this section shall seek to ensure that all people of the United States have access to broadband capability....”).

⁷¹ See Telecom Regulatory Policy CRTC 2009-657, October 21, 2009.

B. No Need for a Strict Scrutiny Standard.

The Coalition is not proposing a strict scrutiny standard by which the FCC must determine that there is only "one way" for a broadband Internet access provider to manage its network to address a legitimate purpose.⁷²

The Coalition also does not endorse a framework where broadband Internet access providers must first seek permission from the Commission to engage in reasonable network management.

OIC supports a flexible framework that can survive advances in technology and changes in Internet usage. Accordingly, OIC does not support detailed, prophylactic network management rules. Instead, OIC urges the Commission to adopt the proposed "Six Principle" framework, which can be enforced on a case-by-case basis as the Commission has done in other contexts.⁷³

⁷² In other words, we can support the Commission's proposal not to adopt the standard articulated in the Comcast Network Management Practices Order. This support is premised on the Commission adopting a general nondiscrimination standard. As discussed elsewhere in this filing, the Coalition believes that the broadband Internet access providers should not discriminate against content, applications, or users. The preservation of a best effort, open Internet through the adoption of a general nondiscrimination principle is critical. We recognize, however, that broadband Internet access providers should have flexibility to manage their network in order to address legitimate network management issues such as addressing congestion or protecting the security of their networks.

⁷³ For example, with respect to the 700 MHz C Block, the Commission's rules simply state that the C Block licensee "shall not deny, limit, or restrict the ability of their customers to use the devices and applications of their choice", subject to reasonable network management, but provides no more detail regarding what

Importantly, it is in the best interests of all Internet stakeholders to respond appropriately to a network that is showing signs of stress, since nothing works well across a congested network. This is why the Coalition recommends the Commission adopt a flexible, nuanced approach that allows broadband Internet access providers to have flexibility to manage congestion and protect their networks.

C. Suggested Framework for Evaluating Reasonable Network Management.

The Open Internet Coalition proposes the following framework to evaluate network management practices.

First, an Internet user would have the burden to bring forward a complaint and make a *prima facie* case that a network management practice

qualifies as limitations or restrictions that would run afoul the rule. Instead, as with the open Internet rules proposed herein, the 700 MHz C Block rules provide an enforcement mechanism that allows the Commission to establish guidelines in an evolving marketplace. See 47 C.F.R. § 27.16.

Other examples in which the Commission has established rules with broadly-worded standards that have been fleshed out through subsequent enforcement and adjudication include the Commissions rules on obscenity and indecency and the requirements that broadcast licensees provide “reasonable access” to Federal candidates and “equal opportunity” to all political candidates. See 47 C.F.R. § 73.3999 (obscenity and indecency), 73.1944 (reasonable access), 73.1941 (equal opportunity).

discriminates against or favors a particular bit of content, an application, or a user, or otherwise violates the rules.⁷⁴

Second, if the complainant makes a *prima facie* case, then the burden would shift to the broadband Internet access provider to demonstrate that the network management practice is meant to address a legitimate purpose.⁷⁵

Third, if the purpose is legitimate, the broadband Internet access provider must demonstrate that the network management practice is narrowly tailored to address such purpose. In determining whether such practice is narrowly tailored, the broadband Internet access provider must—

- demonstrate that the network management practice is designed to address the legitimate purpose and nothing else;
- establish that the network management practice results in as little discrimination or preference as reasonably possible;
- demonstrate that any harm to an end user—including an application or content provider— or to the Internet itself is as little as reasonably possible; and,

⁷⁴ As stated in our discussion about transparency, imposing the burden on a user to make a *prima facie* case is premised on a rule that requires the broadband Internet access provider to disclose its network management practices.

⁷⁵ The Coalition agrees that addressing congestion, blocking spam, blocking malware and similar steps to maintain the proper functioning of a network are legitimate purposes. See *In the Matter of Preserving the Open Internet*, GN Docket No. 09-191; *Broadband Industry Practices*, WC Docket No. 07-52, Paragraphs 138, 140.

· in the case of a technical network management practice, state why network investment or economic network management practices alone would not reasonably further the legitimate purpose.⁷⁶

D. Industry Standards Already Exist for Addressing Congestion.

Today's protocols on the Internet already exhibit congestion-control behaviors. If they did not, the Internet would be regularly collapsing as demand and traffic levels increase exponentially year after year while network upgrades occur on a far less regular basis. If a network product were to be released that always sent at top speed regardless of congestion-control signals, that product would fail to work well because no application works well on a congested path. The traditional and most-used congestion-control algorithm is known as "Additive Increase, Multiplicative Decrease" ("AIMD") behavior. It is designed to expeditiously reduce the rate of sending traffic across a network path that is dropping or delaying packets. Once a rate is found that does not result in signs of congestion, a sender slowly can increase speed to probe for faster send rates that do not create additional congestion.

The Internet Engineering Task Force (IETF) already has deployed a number of solutions available to users and broadband Internet access providers

⁷⁶ A similar test was proposed by the Coalition and adopted by the Canadian Radio-television and Telecommunications Commission. *See* Telecom Regulatory Policy CRTC 2009-657, Paragraph 43. *See also* The Guideline for Packet Shaping, May 2008, P. 7 ("[I]f packet shaping is implemented in such a manner to the extent necessary based on objective data, there is a high possibility that it will generally be regarded as an act performed in the pursuit of a lawful business.

to mitigate and avoid congestion. One example is DiffServ (RFC 2474 et al), where users' applications can help identify traffic that is speed-sensitive. Using DiffServ, broadband Internet access providers can respond, limit by quota, or ignore such instructions. For example, a residential ISP might offer a quota of 180 MB worth of packets marked "EF" (for "Expedited Forwarding") and the user may use them as they see fit. After the quota is exhausted, packets marked EF will be handled using the standard "Best-Effort" handling (the normal neutral Internet behavior toward packets). This leaves users in charge of deciding traffic priority for themselves. While this method has been available for a long time, broadband Internet access providers have yet to offer this well-proven technique to residential end-users. Once they do, applications are likely to be designed to use the markings appropriately. Another example is the numerous congestion control standards and methods already published by the IETF as standards or best current practices.

Following the controversy surrounding Comcast's degradation of the BitTorrent protocol, the IETF began investigating additional techniques, some for broadband Internet access providers, some for end-users and their applications, and some for both, that might result in additional elasticity in links that are awaiting upgrades.

Under the auspices of the Techniques for Advanced Network Applications working group, the IETF is considering proposals that use broadband Internet access provider-supplied information concerning the least-

costly, least-congested route available from or to particular points on its network. This group also will investigate how to use existing technologies such as data caching to reduce the number of far-reaching connections.

While standards bodies such as the IETF can be very helpful in developing consensus-based protocols for handling traffic on the Internet, such bodies are not a substitute for the Commission implementing network neutrality rules.

VIII. THE OPEN INTERNET COALITION STRONGLY OPPOSES THE INCLUSION OF CONTENT FILTERING IN THE SCOPE OF THE DEFINITION OF REASONABLE NETWORK MANAGEMENT

The Open Internet Coalition opposes the Commission's inclusion in the definition of "reasonable network management":

prevent[ing] the transfer of unlawful content or
prevent[ing] the unlawful transfer of content.⁷⁷

The proposed rules would apply only to lawful content.⁷⁸ Of course, this means that the non-discrimination rule applies only to lawful content. The Reasonable Network Management provision works as an exception to the non-discrimination rule, which allows a broadband Internet access provider to discriminate against lawful content in certain situations.

⁷⁷ §8.3(a)(iii) and (iv) of the Draft Proposed Rules for Public Input, Appendix A.

⁷⁸ See, e.g., §8.5, 8.7, 8.9 and 8.13 of the Draft Proposed Rules for Public Input, Appendix A.; *In the Matter of Preserving the Open Internet*, GN Docket No. 09-191; *Broadband Industry Practices*, WC Docket No. 07-52, Paragraph 139.

If the broadband Internet access provider is discriminating against *unlawful* content, the non-discrimination rule does not apply and therefore neither the broadband Internet access provider nor the Commission need worry that blocking the transfer of unlawful content would create jeopardy for the access provider under the rules.

In other words, if a broadband Internet access provider discriminates against unlawful content, there is no need to apply the Reasonable Network Management test because the non-discrimination rule does not apply in the first place.

That leaves the Commission with the possibility that the Reasonable Network Management test could be used to justify discriminating against some *lawful* content in order to prevent the transfer of *unlawful* content. The Open Internet Coalition strongly objects to this possible outcome for several reasons, including –

- (A) It likely would put the rules at odds with specific content-related statutory provisions and frameworks regarding the handling of both lawful and unlawful content;
- (B) It raises the likelihood of a challenge of the rules on Constitutional grounds and the re-application of a strict scrutiny standard the Commission is seeking to abandon; and,
- (C) It possibly violates the federal Wiretap Act;
- (D) It raises substantial privacy concerns;

(E) It violates basic principles of network management by allowing broadband Internet access providers to make sophisticated legal judgments about the nature of content over their networks.

Each of these reasons is explained in greater detail below.

A. It Likely Would Put the Rules at Odds with Specific Content-Related Statutory Provisions and Frameworks Regarding the Handling of both Lawful and Unlawful Content.

Over the years, Congress has passed various statutes that relate to the distribution of unlawful content, and in some cases, specifically relate to the distribution of unlawful content on the Internet. With regard to copyright law, which pertains to the unlawful distribution of lawful content (*i.e.*, the content is legal; the *act* is not), the statutory framework created by Congress is rooted in the First Amendment and the Copyright Clause to the Constitution.⁷⁹

An FCC regime that creates a competing framework to these statutes – and the case law that interprets them – is unnecessary and would invite legal challenges regarding the FCC’s authority to do so. It also would create confusion among stakeholders because of the likelihood of competing and contradictory results relating to the treatment of the same content.

The Commission cites two specific examples of unlawful content or unlawfully transferred content – child pornography and illegally distributed copyrighted works – in its justification for the proposed Reasonable Network Management rule.

⁷⁹ U.S. Const. art. 1, § 8, cl. 8.

In each example, Congress and the courts have created a framework for the treatment of such content.

1. Illegally distributed copyrighted works.

The statutory regime concerning distribution of copyrighted works generally resides in the copyright laws found in Title 17 of the United States Code.⁸⁰ There also are criminal copyright provisions found in Title 18 of the United States Code.⁸¹

Section 106 of the Copyright Act provides certain exclusive rights to the owner of a copyrighted work relating to the reproduction and distribution of a copyrighted work.

The Internet is, among other things, a series of copying machines as it transmits bits of data throughout its networks. It also allows users to receive and share content more quickly and to a wider audience than ever before.

Importantly, the exclusive right in Section 106 is subject to at least two key limitations.

First, Section 107 provides a key limitation on a copyright owner's exclusive right by codifying the privilege of *fair use* of a copyrighted work. Fair use provides important limitations by allowing users in certain situations to distribute protected copyrighted works without authorization from the copyright

⁸⁰ See 17 U.S.C. §§ 501 and 1201

⁸¹ See 18 U.S.C. §§ 2318-2319B.

owner.⁸² As an embodiment of First Amendment rights, the fair use provision in Section 107 allows for unauthorized use of copyrighted works for things such as—but not limited to—criticism, comment, news reporting, teaching, scholarship, or research. In addition, in determining whether other uses of a work are fair use, Section 107 sets forth a flexible four-part test.⁸³

⁸²The Copyright Act's codification of fair use to allow a user to distribute and use copyrighted work without the owner's *authorization* is important. We note that in some rightsholders' statements before the Commission on this subject, the rightsholders claim a right to control distribution, meaning that a work would not be permitted to be distributed without the authorization of the copyright owner. (See, e.g., "In order for legal, licensed platforms for distribution of copyrighted content to be sustainable online, content creators and their distribution partners must curtail the distribution of that same content through unlawful and *unauthorized* web sites, peer-to-peer services, cyberlockers and other online distribution mechanisms." (emphasis added). Comments of the Motion Picture Association of America, Inc., National Broadband Plan for our Future, Notice of Inquiry, GN 09-51, available at <http://fallfoss.fcc.gov/ecfs/document/view?id=7020244174>.)

⁸³The factors in determining whether the use a particular copyrighted work is fair use are —

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107.

This 4-part test has generated a substantial amount of case law interpreting the scope of and interaction between Sections 106 and 107. Thus, the law surrounding these statutes is continually evolving and adapting as they are applied to facts relating to new technologies and uses.⁸⁴ As cases demonstrate, given technological advances, the application of the fair use privilege is routinely tested in the judiciary. The courts – not the Commission – are the arbiters of the four-part test.

Indeed, the U.S. copyright laws delicate balancing of rights and exceptions, as tested and developed by our courts, provides a framework that has enabled entities in the United States to lead the world in the advancement of

⁸⁴ For example, recently the implementation of remote digital video recorder (“R-DVR”) technology offered by Cablevision was challenged by the major motion picture studios (“Studios”). Cablevision offered a technology where the hard drive storing recording programming was not housed at the customer’s premises but rather at Cablevision’s premises. The Studios argued that such Cablevision’s technology constituted a direct infringement of their exclusive rights where Cablevision created unauthorized copies and distributions of Studios’ works, violating § 106 (1), (3). The Studios also claimed that the transmission of the recorded work to the user’s home constituted an unauthorized public performance under § 106(4). Judge Chin of the United States District Court for the Southern District of New York ruled in Studios’ favor. The United States Court of Appeals for the Second Circuit reversed and held in Cablevision’s favor. *See Cartoon Network v. Cablevision*, 536 F.3d 121 (2008), *cert. denied* 129 S. Ct. 2890. This case is a good example of how a new technology raises complex questions of interpretation of Copyright law, which means that Copyright law is continually evolving through occasional Congressional updates to the statute and regularly occurring decisions by our courts. In the Internet and technology space, in almost every instance of a new user technology involving the copying or distribution of content, the Studios challenge such technology under the Copyright laws. *See* <http://arstechnica.com/tech-policy/news/2009/10/100-years-of-big-content-fearing-technologyin-its-own-words.ars>. Last viewed January 14, 2010.

Internet tools, applications, and content. These laws enable the U.S. to lead the world in the Internet ecosystem.

The other important exceptions to a copyright owner's rights are the limitations on liability under the Digital Millennium Copyright Act ("DMCA"), relating to material distributed online.⁸⁵

The DMCA states that an Internet service provider shall not be liable for damages and other relief for infringement insofar as the service provider is engaging in routine activities relating to transmission of third-party content, caching of third-party content, hosting of third-party content, or linking to third-party content.

The exceptions under the DMCA are subject to a delicately balanced statutory regime that requires service providers to comply with such things as a notice-and-take down request from copyright owners and adoption of policies for the termination of repeat infringers.⁸⁶

The framework established under our nation's copyright laws speaks strongly against the FCC establishing a competing framework that permits (and perhaps requires) broadband Internet access providers to prevent the unlawful transfer of content under the Reasonable Network Management section of the proposed rule.

⁸⁵ 17 U.S.C. § 512.

⁸⁶ DMCA, 17 U.S.C. §§ 512(g)(2) and (i)(1)(a).

Congress has clearly occupied the field, and indeed the Constitution vests Congress with the exclusive rights to such occupation.⁸⁷ An FCC framework where the Commission determines what is or is not fair use, who or what is copying or distributing a protected work, or how much lawful content may be blocked in order to prevent either the distribution of unlawful content or the infringing distribution of lawful content falls outside of the FCC's jurisdiction and expertise. Congress has not authorized the FCC to make such decisions, and there is no basis in the Communications Act to argue that the Commission has ancillary authority to allow it to do so.^{88 89}

The Commission does not attempt to make the case that such a framework for the handling of copyrighted works falls under its ancillary authority to a provision in the Communications Act. We believe that is because there is no

⁸⁷ U.S. Const. art. 1, § 8, cl. 8.

⁸⁸ As stated above, even if the Commission had the authority, the proposal raises the likelihood of a competing framework to the copyright laws relating to the handling of the same or similar content.

⁸⁹ The Commission's ancillary jurisdiction is limited to circumstances where: (1) the Commission's general jurisdictional grant under Title I covers the subject of the regulations and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities. See *Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 976 and *Am. Library Ass'n v. FCC*, 406 F.3d 689, 692.

such case to be made. Consequently, in this situation, there is not even a mousehole in which a *mouse* could be hidden.⁹⁰

But because the proposed rules only apply to lawful content, and those rules do not preclude the application of and compliance with content-specific laws, there is no need for the Commission to attempt to conflate copyright and reasonable network management.

Despite the Coalition's skeptical views about whether the FCC should play a role to address these issues through the Reasonable Network Management provision, the Coalition certainly supports the protection of Copyrighted works. The DMCA provides a workable framework for handling unlawfully disseminated copyrighted works.

In addition, there are increasingly promising technical measures and business deals that are allowing edge-based technology companies and content providers to handle the dissemination of copyrighted works.⁹¹ These increasingly innovative solutions at the edges of the network enable creators to

⁹⁰ In the *ALA* case, the D.C. Circuit quoted the Supreme Court in its admonition that Congress "does not . . . hide elephants in mouseholes." See *Am. Library Ass'n*, 406 F.3d at 704, citing *Whitman v. Am. Trucking Ass'n*, 531 U.S. 457, 468 (2001).

⁹¹ For example, even while YouTube is being sued by Viacom for secondary infringement of Copyright, YouTube has developed technologies and partnerships with content providers to handle the posting of protected works that show up on YouTube. Ann Broache and Greg Sandoval, "Viacom sues Google over YouTube Clips, *CNET News*, March 13, 2007. See also YouTube's Content Management Policy available at http://www.youtube.com/t/content_management

monetize content on Web sites and in applications. Increasingly, these technologies will connect users and creators in real time to enable innovative real-time licensing arrangements. Restricting or stopping the flow of bits at the network level would preclude these new, emerging monetization opportunities for artists and creators. The FCC need not enter this arena.

2. Child Pornography Laws.

The Open Internet Coalition looks forward to the day when child pornography is eliminated from the Internet. Many of our members actively work with the National Center for Missing and Exploited Children (“NCMEC”) and law enforcement to identify and eliminate instances of child pornography on the Internet.

Unlike copyrighted works, there are never lawful uses for child pornography. Actual child pornography is not protected speech. However, making the legal determination of what constitutes child pornography is not always easy. Consequently, Congress has created a framework for service providers for handling of electronic dissemination of child pornography, which does not require such providers to make such legal determinations for which the service providers are not qualified.

Under the United States Criminal Code, a service provider providing electronic communication in interstate commerce is required upon learning of an *apparent* violation of criminal statutes relating to the dissemination of child pornography or child exploitation to provide a report to NCMEC. The service

provider also is required to retain relevant information relating to that report for at least 90 days. Upon receiving the report, NCMEC makes a determination whether such report constitutes an apparent violation of the child pornography or child exploitation laws, and forwards such report to the appropriate law enforcement agency.

Next, the law enforcement agency, in its discretion, will normally contact the service provider in order to assemble a case to arrest and prosecute the creator of the illegal content.⁹²

Again, Congress has created a detailed framework for handling of child pornography. The Commission does not have the jurisdiction to create a competing framework, and even if it did, it should not do so.

As in the copyright space, NCMEC and Internet service providers have been working closely on creating technological solutions that would allow such providers to block access to images that have been determined to be child pornography.⁹³ These kinds of technological solutions do not involve the blocking of lawful images. Consequently, a broadband Internet access provider is free to implement this sort of technology without fear of violating any non-

⁹² See 18 U.S.C. § 2258A.

⁹³ See, e.g., http://missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageID=3644.

discrimination provision. Thus any need to address this through the reasonable network management exception is misplaced.

B. It Raises the Likelihood of a Challenge of the Rules on Constitutional Grounds.

Even if the Commission could find the ancillary authority to regulate the dissemination of copyrighted works, such a framework raises the likelihood of a challenge on Constitutional grounds. As noted above, the only need for the Reasonable Network Management rules relating to unlawful content would be in order to create a framework that would allow broadband Internet access providers to block some lawful content. The FCC's authorization of blocking of a protected copyrighted work that falls under the fair use exception to Section 107 of the Copyright Act, for example, would likely violate the First Amendment of the U.S. Constitution.

As the Supreme Court has noted, the monopoly afforded authors over their works through copyright protection is Constitutional because of the twin escape valves of fair use and the fact that copyright does not protect ideas or facts contained in a copyrighted works.⁹⁴ These twin escape valves are rooted in the First Amendment to the Constitution, prohibiting Congress from adopting laws that infringe upon freedom of speech.⁹⁵ In addition, any filtering mechanism employed at the network level undoubtedly will capture non-infringing material besides material protected by fair use or facts, including

⁹⁴ *Eldred v. Ashcroft*, 537 U.S. 186, 219-220 (2003).

lawfully distributed licensed materials, public domain material, and material created by users and filtered erroneously.

A framework that authorizes blocking of such lawful distribution of works essentially would constitute a prior restraint on users' rights under the First Amendment.

In addition, the scrutiny a court would apply to such content regulation would be the traditional strict scrutiny standard that the First Amendment requires, putting the Commission right back in the position of having a Reasonable Network Management regime that would be a strict scrutiny regime.

Instead, the Commission can remove itself from having a regulatory structure that determines what lawful content is permissible to block by removing the two prongs of the Reasonable Network Management test that would authorize the blocking of lawful content.

C. Inspection of Content for Legality May Violate the Federal Wiretap Act.

The federal Wiretap Act, as amended by the Electronic Communications Privacy Act, protects a user's electronic communications.⁹⁶ Specifically, the relevant provision states—

[A] person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any

⁹⁵ U.S. Const. amend. I.

⁹⁶ 18 U.S.C. §§ 2510-2522.

communications...while in transmission on that service to any person other than an addressee or intended recipient....”

18 U.S.C. § 2511(3)(a).

The Act also prohibits the “interception” of electronic communications, which are defined as the “acquisition of the contents of any ... electronic ... communications through the use of any electronic, mechanical, or other device.”⁹⁷

There are exceptions to these prohibitions. The most relevant exceptions for the purpose of this discussion are an exception for cooperating with law enforcement requests and an exception when the user provides consent to the interception or divulgence of the user’s communication.

The law enforcement exception is at issue here, because the Reasonable Network Management provision has a separate section relating to appropriate requests by law enforcement. While there is not a lot of case law about what exactly would constitute appropriate consent, current case law suggests that consent must be actual (as opposed to constructive) and that the user knows exactly what he or she is consenting to in each instance of interception or divulgence.⁹⁸ Given broadband Internet access providers’ compliance with the Wiretap Act, which the proposed rules contemplate, there is no need to address

⁹⁷ *Id.* at 2519(4).

⁹⁸ See, e.g., *Griggs-Ryan v. Smith*, 904 f.2d 112 (1st Cir. 1990), *In re Pharmatrak v. Privacy*, 329 F.3d 9 (1st Cir. 2003), *Berry v. Funk*, 146 F. 3d 1003 (D.C. Cir. 1998).