

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

Preserving the Open Internet

GN Docket 09-191

Broadband Industry Practices

WC Docket No. 07-52

**COMMENTS OF THE  
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION  
(CCIA)**

Edward J. Black  
Catherine R. Sloan  
Matthew C. Schruers  
CCIA  
900 17th Street, N.W.  
Suite 1100  
Washington, D.C. 20006  
Tel. (202) 783-0070  
Facsimile (202) 783-0534  
Email: EBlack@ccianet.org  
CSloan@ccianet.org  
MSchruers@ccianet.org

Jonathan E. Canis  
Stephanie A. Joyce  
G. David Carter  
Arent Fox LLP  
1050 Connecticut Avenue, N.W.  
Washington, D.C. 20036  
Tel. (202) 857-6000  
Facsimile (202) 857-6395  
Email: Canis.Jonathan@arentfox.com  
Joyce.Stephanie@arentfox.com  
Carter.David@arentfox.com

*Counsel to CCIA*

Dated: January 13, 2010

## TABLE OF CONTENTS

SUMMARY .....	1
I. INTRODUCTION: THE COMMISSION HAS AN OPPORTUNITY NOW TO ADDRESS NEW TECHNOLOGIES THAT GIVE OPERATORS UNPRECEDENTED CONTROL OVER INTERNET TRANSMISSIONS .....	2
II. ADOPTION OF OPEN INTERNET ACCESS RULES WILL ENSURE THAT NETWORK OPERATORS HAVE INCENTIVES TO ACT IN A FAIR AND PROCOMPETITIVE MANNER.....	7
III. ALLOWANCE FOR “REASONABLE NETWORK MANAGEMENT” SHOULD BE CAREFULLY CIRCUMSCRIBED .....	10
A. “Reduce or Mitigate the Effects of Congestion on Its Network or to Address Quality-of-Service Concerns”.....	12
B. “Traffic That Is Unwanted by Users or Harmful” .....	18
C. “Prevent the Transfer of Unlawful Content” and “Prevent the Unlawful Transfer of [Lawful] Content” .....	20
1. Because the first five principles as articulated in the NPRM are limited to lawful conduct, the question of law enforcement and civil dispute adjudication is not relevant to “reasonable network management.” .....	21
2. Even if unlawful content, services, and applications were germane to the NPRM, law enforcement is not network management. ....	22
3. Conflating network management with the adjudication of civil disputes and criminal matters would usurp the role of the federal judiciary and constitutes bad policy.....	22
4. Recommendations for Final Rule .....	24
a) The definition should not confuse “allegedly unlawful” and “unlawful.” .....	24
b) The definition should not confuse civil disputes and criminal law.....	25
c) The definition should not confuse the transfer of unlawful content with the unlawful transfer of lawful content. ....	25

d)	The final rule should state that the antidiscrimination rules are subject to the needs of law enforcement officials, rather than the more amorphous “law enforcement.” .....	27
D.	Addressing Law Enforcement, Public Safety, and Homeland and National Security Concerns .....	28
IV.	NETWORK OPERATORS AND IAPS SHOULD BE REQUIRED TO PUBLISH ALL NETWORK MANAGEMENT PRACTICES, TERMS OF SERVICE, AND RESTRICTIONS CLEARLY AND CONSPICUOUSLY TO CONSUMERS .....	30
V.	THE COMMISSION SHOULD ESTABLISH AN ADVISORY PANEL AS THE TRIBUNAL OF FIRST RESORT FOR THE ENFORCEMENT OF ANY NEW RULES OR GUIDELINES.....	34
	CONCLUSION.....	38
ATTACHMENT A	Kip Meek & Robert Kenny, Ingenious Consulting Network, “Network Neutrality Rules in Comparative Perspective: A Relatively Limited Intervention in the Market” (January 2010)	

The Computer & Communications Industry Association (“CCIA”), by and through counsel, files these Comments in response to the Notice of Proposed Rulemaking released October 22, 2009, in these dockets (“NPRM”). These comments address the principles of open Internet access that the Commission articulates in the NPRM and explain that the Commission’s goals have been and will continue to be attained by adopting a regulatory construct that focuses on consumer choice, the clear disclosure of terms of service and network practices, and industry involvement in crafting and enforcing necessary rules.

### **SUMMARY**

An open Internet is thriving in America as application and content providers have burgeoned to meet longstanding consumer and business demand. The success of the Internet is attributable to Congress’s and the Commission’s moderate regulatory approach paired with measured responses to demonstrated malfeasance. Such restraint remains appropriate and can be maintained without compromising the integrity of networks or intellectual property.

Subscriber preferences, in both content choice and traffic prioritization, should be fiercely protected in the upcoming rules, because they remain the most transparent indicia of demand in a competitive market. Moreover, subscriber preferences most closely comport with the Commission’s focus in the NPRM on the user, rather than the regulator or network operator, as the best arbiter of Internet demand. Where subscriber preferences create a clear and present danger to network integrity, Internet access providers (“IAPs”) of course must have some authority to curtail them. This authority, however, should be circumscribed by rules that require IAPs to have some demonstrable network need and to employ a reasonably tailored means of addressing that need. In further keeping with this focus on subscriber preferences, but recognizing the Commission’s desire

to encourage investment, CCIA agrees that tiered pricing based on bandwidth usage is an appropriate tool for regulating, in a market-driven way, Internet traffic flow.

The Commission also should be mindful of the several legal regimes already in place regarding unlawful content and unlawful transmissions. Intellectual property rights, for example, are protected over Internet transmissions via the Digital Millennium Copyright Act. CCIA would urge the Commission to be cautious not to establish a new layer of regulation in areas beyond its expertise and statutory jurisdiction.

Finally, enforcement of the forthcoming open Internet access rules should be accomplished through a somewhat new rubric than what is now applied to intercarrier disputes. The Commission's resources already are taxed to an extraordinary degree, and its existing enforcement protocol — involving full evidentiary proceedings — is perhaps too blunt a force to employ in the first phase of an open access dispute. A new open Internet complaint process incorporating the Chief of the FCC's Consumer Protection Bureau and a technical advisory board, which amasses the expertise of the FCC, industry engineers, and policy experts, could be a more efficient tribunal of first resort for such disputes. This panel, analogs of which already are used in other contexts, would decrease significantly the burden on the Commission of conducting complaint proceedings until this technical board can vet, review, and craft recommendations for addressing open access disputes.

**I. INTRODUCTION: THE COMMISSION HAS AN OPPORTUNITY NOW TO ADDRESS NEW TECHNOLOGIES THAT GIVE OPERATORS UNPRECEDENTED CONTROL OVER INTERNET TRANSMISSIONS**

The Internet is an undeniable success. It is no overstatement to say that the Internet has fomented a communication and commercial revolution. It is likewise no overstatement to opine that the Internet provides a valuable, possibly unique case study of how competition and

growth can be attained and maintained in new markets. Because both Congress and the Commission have employed a palpable restraint in regulating the Internet,<sup>1</sup> all facets of society have, however unintentionally, worked together to create a free, robust, and virtually limitless online environment.

The Commission is of course aware that access to last mile facilities, particularly broadband facilities, thus far has been the only significant barrier to Internet participation.<sup>2</sup> Public access to those critical local network facilities has always been subject to some level of federal, state, and local regulation. CCIA is confident that the Commission's work in constructing the National Broadband Plan will increase dramatically the ability of every American to obtain affordable and reliable broadband Internet access. Open Internet rules can only further this objective, because broadband adoption is more likely to occur when subscribers can be assured that Internet access will indeed allow them to reach all content, services, and applications available on the Web, not just some subset preselected or favored by their IAP.<sup>3</sup>

---

<sup>1</sup> *E.g.*, NPRM ¶ 47 (“it has long been U.S. policy to promote an Internet that is both open and unregulated”).

<sup>2</sup> *See, e.g.*, GN Docket No. 09-51, Comments of the Computer & Communications Industry Association at 7-9 (June 8, 2009).

<sup>3</sup> The U.S. Department of Justice recently acknowledged the importance of the availability of content and applications:

Other important elements of the ecosystem are the content and applications available, the devices that consumers use to receive, process, and display that content and those applications, and consumers' familiarity with and skill in using computers and the Internet. ... In formulating policies to encourage the adoption and affordability of services, the FCC needs to consider not only the number and characteristics of existing and future providers but also how these complementary inputs impact the goals the FCC seeks to achieve.

For purposes of this proceeding, the danger facing open Internet access lies in network management technology that has become increasingly sophisticated and available. Deep Packet Inspection (“DPI”) software now gives network operators the ability to identify, prioritize, block, and retard data transmissions at the bit level.<sup>4</sup>

These technologies could compromise not only open Internet access but Internet user privacy as well. DPI software already is used at the network level to conduct behavioral advertising, a practice which members of Congress<sup>5</sup> and the Federal Trade Commission<sup>6</sup> have attempted to curtail. The European Union is likewise concerned, and in April 2009 commenced an infringement proceeding against the United Kingdom for permitting the use of “Phorm” behavioral advertising software.<sup>7</sup> The same DPI technology under scrutiny in the advertising context can be

---

GN Docket No. 09-51, *Ex Parte* Submission of the United States Department of Justice at 4, 5 (Jan. 4, 2010) (“DOJ *Ex Parte*”).

<sup>4</sup> Deep Packet Inspection is the act of any IAP’s network equipment, which is not an endpoint of a communication, using any field other than the delivery instructions of the packet for any purpose. Deep Packet Inspection technology enables an IAP to know the contents of a user’s transmission and can be used for data mining, eavesdropping, and censorship. *See* Opening Statement of Dr. David P. Reed, MIT Communications Futures Program, at the Federal Communications Commission’s Public Hearing on Broadband Network Management Practices at Harvard Law School (Feb. 25, 2008) (“Reed Testimony”).

<sup>5</sup> Representative Ed Markey (D-MA) and Representative Joe Barton (R-TX) launched a joint investigation in 2008, including issuing 33 letters of inquiry, regarding the use of software to track Internet users’ activity on the Internet. *E.g.*, “Markey Pushes for Online-Privacy Legislation,” *Broadcasting & Cable* (July 17, 2008), *available at* <[http://www.broadcastingcable.com/article/114606-Markey\\_Pushes\\_for\\_Online\\_Privacy\\_Legislation.php?>](http://www.broadcastingcable.com/article/114606-Markey_Pushes_for_Online_Privacy_Legislation.php?>); “Some Web Firms Say They Track Behavior Without Explicit Consent,” *Wash. Post* (Aug. 12, 2008), *available at* <[>](http://www.washingtonpost.com/wp-dyn/content/article/2008/08/11/AR2008081102270.html).

<sup>6</sup> FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), *available at* <[>](http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf).

<sup>7</sup> IP/09/570, Telecoms: Commission launches case against UK over privacy and personal data protection (Apr. 14, 2009), *available at* <[>](http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en).

used to monitor and impede Internet use; the Commission has an opportunity in this proceeding to adopt rules prohibiting use of DPI in an unjust, discriminatory or unreasonable manner.

From the outset, CCIA states that it fully supports the Commission's adoption of the six principles outlined in the NPRM. CCIA is particularly pleased that the Commission has built on the four principles in Chairman Powell's *Internet Policy Statement*<sup>8</sup> to add express requirements for nondiscrimination and transparency of network practices. Codification of these principles is a necessary and appropriate step in ensuring that the Internet remains an open, competitive environment as the market structure of access, application, and content providers begins to take more definite shape. This action is exactly in keeping with the Commission's longstanding policy of minimal intrusion and measured regulation of Internet access services.

These comments focus on the degree to which it is necessary to qualify the six principles that would allow Internet access providers ("IAPs") to maintain control over traffic flow on the basis of technical network management practices. Though CCIA recognizes that the first responsibility of network operators is to protect the integrity of their facilities, an unfortunate potential for abuse lies in any rule that enables an operator to restrict Internet traffic based on what could be unfounded network concerns. Because each IAP has a "terminating access" monopoly on the physical conduit for any and all information and services from the Internet to reach its own subscribers, those subscribers need certain public interest protections. This is true even if a subscriber has one or more other IAPs from which to choose service. In addition, CCIA strongly rejects any suggestion that the Commission should establish a new layer of content-based regulation in addition to existing safeguards, such as the Digital Millennium Copyright Act, 17

---

<sup>8</sup> *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities*, CC Docket Nos. 02-33, *et al.*, Policy Statement, 20 FCC Rcd. 14986 (2005).

U.S.C. § 512, or indeed that either the Commission or the IAPs are the best arbiters of what is “unlawfully transmitted” content.

Because of the advent of DPI and other network management technologies, the “reasonable network management” caveat to the six principles is particularly portentous. As CCIA explains in Section III. herein, the Commission should be cautious in empowering IAPs unilaterally to set prioritization under the guise of network integrity and potential unlawful transmission of content. “Reasonable network management” can become a “Trojan horse” that dominant IAPs could use to cloak discriminatory or unreasonable practices. At this stage of the Internet’s development, the Commission has enough information about the structure of the telecommunications market — particularly the ownership and deployment of transmission infrastructure — to craft a clear delineation between what is presumptively reasonable and what is presumptively unreasonable.

Above all else, the Commission should empower Internet users as much as possible to decide how their IAP should handle their Internet traffic, rather than allow the IAP to impose its practices on its end users. As the NPRM states, the rules should “protect and empower consumers” and “maximize the efficient operation of relevant markets.” NPRM ¶ 118. This goal is best accomplished by adherence to the Commission’s newly proposed sixth principle: transparency. *Id.* ¶¶ 118-132. The Commission should adopt its tentative rule requiring IAPs to disclose their network management practices to Internet users as well as other content, application, and service providers. *Id.* ¶¶ 121-127. As the oft-quoted Justice Brandeis said, “sunshine is the best disinfectant.”

## **II. ADOPTION OF OPEN INTERNET ACCESS RULES WILL ENSURE THAT NETWORK OPERATORS HAVE INCENTIVES TO ACT IN A FAIR AND PROCOMPETITIVE MANNER**

American competition law is grounded in the belief that open markets are the most developed and efficient markets. The Internet is an archetype of this principle. In the NPRM, the Commission displays an acute awareness of this fact. *See generally* NPRM ¶¶ 28-49. The key, then, in this proceeding is for the Commission to adopt a regulatory framework which continues to encourage openness and innovation.

The Commission recognizes that providers of Internet access, as opposed to competitive online applications and services, retain significant control over both the supply and demand sides of Internet usage. NPRM ¶¶ 67-74. That is, Internet access providers, by virtue of their control over last-mile facilities and the customer relationship, have the ability to regulate the content made available to users as well as users' ability to access content. *Id.* ¶¶ 71, 74. This is the so-called "terminating access" monopoly. Where the relevant firms are dominant or are vertically integrated, or both, that ability often translates into conduct. *Id.* At this juncture in the Internet's short lifespan, the question arises whether sufficient market forces exist to neutralize the recent convergence of increased carrier consolidation and integration, last-mile broadband market power, and unprecedented sophistication of network management technologies.

CCIA believes that codifying an open Internet access regime is the best solution for guiding existing market forces in a manner that encourages investment, innovation, and subscription. Clear rules of the road provide greater certainty; suppliers and purchasers are best able to make choices when the results of those choices have predictable outcomes. In its recent

paper “Free to Invest: The Economic Benefits of Preserving Net Neutrality,”<sup>9</sup> Inimai Chettiar and J. Scott Holladay of the Institute for Policy Integrity posit a similar theory: “From an economic standpoint, the goal of federal government Internet policy should be to maximize the net present value of the Internet.” They discuss “net neutrality” as a “tradeoff of wealth” between IAPs and content providers — IAP subscription models and practices can affect the ability of content providers to reach the market and maximize their return. The paper thus targets the Commission’s core mission in this proceeding which is to craft incentives for maximizing the value propositions of the Internet rather than limiting them through excessive intervention. *See* NPRM ¶¶ 51-55.

CCIA has commissioned a study by Ingenious Consulting discussing pertinent examples of regulatory intervention in new and developing markets in other countries around the world. Kip Meek & Robert Kenny, “Network Neutrality Rules in Comparative Perspective: A Relatively Limited Intervention in the Market” (January 2010) (**Attachment A**) (“Net Neutrality Paper”). Drawing largely from member nations of the Organisation for Economic Co-operation and Development (“OECD”), this study analyzes various forms of non-price market regulation as to their policy bases, objectives, and ability to incentivize firms to act in a nondiscriminatory, procompetitive manner. It then compares these forms of non-price regulation with the prevailing regulatory climate in the United States, including the Commission’s open Internet proposal here, as to their relative intrusiveness and perceived success.

The most notable conclusion in the Paper is that the United States has proposed the mildest form of market regulation of the dozens of nations studied. Net Neutrality Paper at 23, Figure 3. Whereas 23 nations have adopted some form of separations, ranging from accounting

---

<sup>9</sup> “Free to Invest” at 5. Released January 7, 2010; *available at* <[http://policyintegrity.org/documents/Free\\_to\\_Invest.pdf](http://policyintegrity.org/documents/Free_to_Invest.pdf)>.

separations to wholesale-retail structural separation, the United States has engaged in, according to the Paper, “the mildest regulatory interventions to address the access bottleneck.” *Id.* at 33. This restraint thus far has proven successful, largely because innovation and intermodal competition have exerted more force than could any desire to engage in exclusionary conduct. *See generally id.* at 24-29. Should the IAP market become more prominently dominated by a small cadre of firms, or if those firms exhibit further vertical integration, America’s felicitous experience with these “mild” interventions may sour.

As the Commission is aware, many IAPs have suggested that regulatory intervention in Internet access will remove their incentives to innovate and expand. *See NPRM* ¶ 65. CCIA believes, however, that adoption of open Internet access rules will foster innovation and expansion. If all Internet actors collectively are prohibited from arbitrarily restricting Internet usage and compromising access to content, then all Internet actors will have an incentive individually to maintain the least restrictive management policies that they can. Any restrictions based on network management concerns would be as narrowly curtailed as possible. In this way, the Commission can create a regime in which its goals for preserving an open, robust Internet align directly with each IAP’s incentive to maximize value propositions related to the utilization of its network.

It bears mention that the IAPs’ suggestion that increased regulation necessarily will stifle innovation illustrates the potential for anticompetitive conduct in the Internet market as presently structured. It is the IAPs, along with a few providers of wholesale backbone, who thus far have “built” the Internet facilities infrastructure we enjoy today; in predicting the demise of an open Internet, the IAPs reveal the degree to which they are able to control its preservation. If intended as a threat, this threat has power only because the IAPs do.

CCIA notes, however, that the Department of Justice has elsewhere suggested that it is not particularly useful to debate the extent to which the broadband access marketplace is not competitive or oligopolistic. Rather, obvious duopoly conditions involving huge dominant providers enjoying economies of scale suggest the need for policies to improve consumer outcomes.<sup>10</sup> Nonetheless, given the market structure of last mile facilities today — essentially a duopoly between cable and wireline facilities (DSL and fiber) — and the network management technologies, like DPI, being deployed, the Commission should address this question now by adopting the six principles in the NPRM.

### **III. ALLOWANCE FOR “REASONABLE NETWORK MANAGEMENT” SHOULD BE CAREFULLY CIRCUMSCRIBED**

The Commission has proposed to affix to each of the proposed six net neutrality principles a qualifier stating that the principle would give way to “reasonable network management” practices. The Commission proposes that “reasonable network management” be defined as:

- (a) 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) to

---

<sup>10</sup> We do not find it especially helpful to define some abstract notion of whether or not broadband markets are “competitive.” Such a dichotomy makes little sense in the presence of large economies of scale, which preclude having many small suppliers and thus often lead to oligopolistic market structures. The operative question in competition policy is whether there are policy levers that can be used to produce superior outcomes, not whether the market resembles the textbook model of perfect competition. **In highly concentrated markets, the policy levers often include: (a) merger control policies; (b) limits on business practices that thwart innovation (e.g., by blocking interconnection); and (c) public policies that affirmatively lower entry barriers facing new entrants and new technologies.**

DOJ *Ex Parte* at 11 (emphasis added).

prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content; and (b) other reasonable network management practices.<sup>11</sup>

The Commission requests comment on the specific wording of the proposed definition of “reasonable network management.”<sup>12</sup> The Commission also seeks comment regarding how to evaluate whether a particular network practice falls into the definition of “reasonable network management” and who should bear the burden of proof.<sup>13</sup> Further, the Commission seeks comment on whether third parties, such as the Internet Engineering Task Force (IETF), should play a role in defining more precisely what practices are reasonable and whether the transfer of particular content is unlawful.<sup>14</sup>

CCIA, like other previous commenters, is concerned that this Commission’s proposed “reasonable network management” qualifier may become a subterfuge by which the desired net neutrality protections will be eviscerated.<sup>15</sup> CCIA thus encourages the Commission to provide greater certainty to IAPs with regard to what will be considered a “reasonable network management” practice, or, perhaps more precisely, what will *not* be considered reasonable, in order to provide the industry with greater certainty and uniformity. As discussed more fully

---

<sup>11</sup> NPRM ¶ 135.

<sup>12</sup> NPRM ¶ 141.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *See, e.g.,* Barbara van Schewick, Official Testimony at the Federal Communications Commission’s Second Public *En Banc* Hearing on Broadband Network Management Practices at Stanford University (Apr. 17, 2008) (“van Schewick Testimony”) (“Without [ground] rule[s], ‘reasonable network management’ becomes the back door that enables network providers to undermine the non-discriminatory nature of the Internet that the FCC’s Internet Policy Statement is designed to protect.”).

below, CCIA believes that the Commission’s case-by-case adjudicatory process is ill-suited to provide the industry with clear guidance and that a dedicated technical advisory organization should be formally designated to establish these standards.

**A. “Reduce or Mitigate the Effects of Congestion on Its Network or to Address Quality-of-Service Concerns”**

The Commission correctly observes that “the general usefulness of the Internet could suffer if spam floods the inboxes of users, if viruses affect their computers, or if network congestion impairs their access to the Internet.” NPRM ¶ 133. To this end, CCIA is not opposed to the IAPs’ continuing to take reasonable pro-active technical measures to curtail harmful viruses and reduce or minimize spam. However, the Commission should approach any complaints about network congestion as the basis for tough network management practices with caution. Of course, in general, the best response to network congestion is to upgrade network capacity, rather than manage artificial scarcity. This may be a very tall order for some wireless carriers, given the shortage of available spectrum, but the principle remains a valid and fundamental one.

Importantly, the Commission should seek to ensure that *subscribers* — consumers and small businesses — have the opportunity to make informed decisions about broadband Internet access. And the Commission should seek to protect subscribers by guarding against IAPs that might allow their network capacity to degrade by relying too heavily on network management practices rather than making appropriate infrastructure investment and upgrades. The Commission must ensure that the nation’s broadband infrastructure remains ready to meet subscribers’ evolving needs.

CCIA also believes that subscriber preference should be the guiding force in traffic prioritization. In particular, the Commission should create a safe harbor provision that ensures IAPs that their network management practices will be deemed presumptively reasonable if the

IAP: (1) apportions each end user a proportional share of bandwidth on the network at any given time; and (2) enables each end user the opportunity to select how its traffic is prioritized within its share of bandwidth. In this manner, the IAP could have a default prioritization scheme, but a subscriber could decide whether to prioritize his VOIP traffic over his video-downloading traffic and over his general web browsing.<sup>16</sup> Recognizing that a one-size-fits-all approach to traffic prioritization is a disservice to subscribers, and that each subscriber should be empowered to customize his or her Internet experience based on his or her given needs, will help to ensure that innovation is not stymied.

Once a subscriber has stated his traffic prioritization preferences, the IAP's chief role is to implement them. CCIA acknowledges, however, that an IAP may need to conduct independent traffic prioritization in order to comport with and protect subscriber preferences. That is, it would be acceptable for an IAP to prioritize traffic such that the subscriber's most latency-intolerant uses, such as voice communications, are prioritized over the subscriber's least latency-intolerant uses, such as obtaining entertainment content. Any such independent prioritization must flow directly from the subscriber's own usage choices and preferences. Moreover, as discussed in fuller detail below, CCIA believes it is important that any such practices be adequately disclosed in order that subscribers can understand how the IAP will make decisions which will affect their user experience on the Internet.

Another important consideration in the discussion about allowing IAPs to use network management principles to ease congestion should be a countervailing desire to ensure that subscribers continue to receive the benefit of their bargain. For example, if a consumer subscribes for broadband service from a provider that is advertising 6 MB download/1 MB upload at the time

---

<sup>16</sup> See van Schewick Testimony at 7.

of subscription, the consumer should have some expectation that its service will not be significantly degraded while the consumer continues to pay the monthly subscription fee. In essence, subscribers expect that they are contracting for a minimum quality-of-service level and IAPs should not be allowed or encouraged to use network management practices as a substitute for maintaining the integrity of the network. Nor should IAPs be permitted or encouraged to allow their networks to degrade in order to then “upsell” subscribers to return to the quality of service for which they initially contracted.

This is not to suggest, however, that CCIA is opposed to having tiered or usage-sensitive pricing structures. *See* NPRM ¶ 65. Indeed, CCIA generally agrees that subscribers should pay for the services that they receive. CCIA would support IAPs that implement either usage-sensitive or usage-and-time sensitive pricing models. In this way, users that are “bandwidth hogs,” those who use tremendous bandwidth by constantly playing video games, watching IPTV, and the like, do not impose externalities on other Internet users through their bandwidth-intensive applications. Similarly, time-sensitive fees for peak time usage, similar to those utilized by many wireless carriers, which might provide, for example, free nights and weekends for wireless customers, is an appropriate market-driven solution to network congestion concerns. This concept **does not** contemplate time-sensitive or per-minute metering, but rather throughput-sensitive metering where a subscriber exceeds his subscribed bandwidth amount. Here again, the focus is on putting the choice in the hands of subscribers, and not deputizing IAPs to control the content or the manner in which subscribers use the Internet.

Subscriber choice may, of course, be monetized and strictly followed. That is, it would not be unfair or discriminatory to couple a tiered pricing structure with a practice which, when a subscriber exceeds his requested bandwidth, imposes additional fees for that overage. This

practice is much like the typical practice in the wireless PCS industry: when one exhausts their allotted minutes, a higher per-minute rate applies. Such fees may be applied only if the IAP gives the subscriber **clear and conspicuous notice** and implements the fee on a fully content-neutral and technology-neutral basis. Subscriber agreements should state explicitly that exceeding one's bandwidth tier will result in overage fees of a defined amount. As CCIA consistently maintains throughout these comments, the key to any open Internet regime lies in full disclosure of all rates, terms, and conditions.

It also would be appropriate to permit IAPs to implement a bandwidth cap that would prevent subscribers from exceeding their allotted throughput. For example, parents may wish to prevent incurring additional fees in the event that their children attempt to use Internet-based applications that greatly increase bandwidth usage. IAPs could offer the bandwidth cap as a service feature, and in this way meet subscribers' needs while also protecting network integrity. Any such device should, however, be permitted only on an "opt in" basis — the account holder must evidence an affirmative choice to cap their own bandwidth use.

With regard to wireless broadband access, CCIA suggests that the six principles articulated in the NPRM are appropriate, though a certain degree of modification is warranted to address the particular limitations of wireless transmissions. Access to the Internet over both mobile and fixed wireless broadband networks raises unique considerations, as recognized by the Commission. NPRM ¶¶ 163-170. CCIA acknowledges that mobile wireless networks, and to a lesser extent fixed wireless networks, face much greater capacity constraints than wireline networks, and face signal interference issues that do not arise with wireline networks.<sup>17</sup> As such,

---

<sup>17</sup> The bandwidth overage fee and bandwidth cap concepts, for example, may be unworkable in a pure point-to-point wireless network due to limitations in the ability to manage wireless spectrum use at the subscriber level.

the need for effective network management for wireless networks may be greater, and may merit special consideration. At the same time, however, iPhones, smartphones, and other CMRS handsets are already one of the most widely used means of accessing the Internet, and this data usage is growing dramatically.

It is therefore apparent that failure to apply the Commission's six open Internet principles to 3G and 4G wireless networks would deny critical protections to one of the of the largest vehicles — and the fastest-growing vehicle — for obtaining high-speed access to the Internet in this country. A recent report by the Center for Disease Control shows that, in 2007, 16% of U.S. adults — 32 million people — terminated their landline phone service and replaced it with cellular service. This pattern is up from 5% in 2004. Given this explosive growth, the Commission cannot exclude this sector of the Internet-using public from its open Internet policies.

Moreover, two of the largest CMRS carriers and spectrum holders in the country are affiliates of the largest IAPs. As a result, the same concerns CCIA has identified regarding the ability of the dominant IAPs to manipulate the proposed principles to disadvantage competitors and to avoid necessary network investment applies with equal force to the largest CMRS providers.

The NPRM specifically seeks comment on whether “tethering” should be required as a form of device interconnection. Tethering is the ability of a wireless handset or other device to act as a modem to allow interconnectivity to other devices. NPRM ¶¶ 164-69. CCIA believes that tethering can be extremely beneficial, and can provide wireless subscribers with dramatically increased functionality. As the Commission notes, it is now common for dual-mode and multi-mode handsets to enable the interconnection of devices on CMRS and Wi-Fi networks. NPRM ¶ 164. This cross-networking allows both the subscriber and the service provider to realize a

“network effect” that increases the value of the service. Interconnectivity ensures, for example, that a subscriber to AT&T Wireless CMRS service can call, and receive calls from, a subscriber to T-Mobile CMRS service. This increases the value of the services to AT&T, T-Mobile, and their respective subscribers. This same network effect will be realized as subscribers to CMRS service increasingly can access users of services on other networks, such as Wi-Fi or WiMAX-based networks.

At the same time, CCIA is cognizant of legitimate wireless carrier concerns over network management requirements and interoperability standards. Rather than establish a “one size fits all” rule regarding tethering, CCIA proposes that the Commission establish a preference in favor of tethering. Once established, the application of the other safeguards proposed by CCIA — the publication of carriers’ network management policies in clear and unambiguous terms, the guarantee of nondiscriminatory apportionment of bandwidth among a network’s users, and the establishment of a dedicated technical advisory organization — can ensure that this preference for tethering is implemented in a reasonable and responsible manner.

In addition, the NPRM notes that the proposed six principles actually impose a less stringent set of network-sharing and interoperability requirements than the rules adopted by the Commission for its Upper 700 MHz C Block licensees. NPRM ¶ 169. CCIA again believes that it is not necessary to impose a “one size fits all” answer to this question. Rather, the application of the six principles, along with the additional safeguards proposed by CCIA in these Comments, can determine whether and to what extent departure from the existing rules is necessary. With the assistance of a dedicated technical advisory body, the Commission can determine if forbearance from enforcing existing rules is appropriate.

**B. “Traffic That Is Unwanted by Users or Harmful”**

The second prong of the Commission’s proposed definition for reasonable network management states that it would be reasonable for an IAP to use network management technology to “address traffic that is unwanted by users or harmful.” NPRM ¶ 135. CCIA agrees, in principle, with the Commission that IAPs should be able to address traffic that is unwanted by users or harmful to the network. As with the previous discussion, CCIA encourages the Commission to ensure that individual choice is heard and that the preferences of the many do not become the *de facto* choice for all subscribers.

The *Comcast Network Management Practices Order* also brings to light two important practices that the Commission should be extremely focused on as it considers the future of the Internet: DPI technology and RST Injection.<sup>18</sup> CCIA believes that IAPs should use DPI technology sparingly, if at all. While DPI may provide benefits for controlling and curtailing spam, Internet users generally do not anticipate that their broadband access provider will be examining the contents of their transmissions. To use an apt analogy from the Commission’s *Comcast Network Management Practices Order*, subscribers view IAPs as mail carriers. The consumer addresses his/her letter, places postage on the envelope, and anticipates that the mail carrier will deliver the package *unopened* to its destination. CCIA would not expect that the mail carrier will use steam to open the mail, read the letter, and then try to reseal the envelope. Indeed, any mail carrier that does open the mail, absent some court order, will quickly find themselves in

---

<sup>18</sup> Reset Packet or RST Injection is a process by which an IAP falsifies network traffic by sending a reset packet to another computer on the network. The reset packet signals that something has gone wrong in the transmission of the network and stops the current packet flow. See Reed Testimony.

jail.<sup>19</sup>

CCIA believes that the same standard generally should apply to IAPs. And, to the extent that there are “critically important” reasons to monitor user content, such as the elimination of harmful traffic, for which the use of DPI can be “narrowly or carefully” tailored, CCIA believes that IAPs should be required to notify subscribers clearly about the use of DPI and the limited purposes for which DPI will be used on the network.

With regard to RST Injections, CCIA presently believes that a bright line rule is desirable. CCIA can think of no situation in which the use of RST Injection, or the falsification of any network data, is a desirable or appropriate form of network management.<sup>20</sup> Indeed, the notion that RST Injections should be used as a network management technique has been rejected by researchers in the field.<sup>21</sup> To the extent IAPs believe that there are necessary and legitimate reasons to falsify network traffic, that matter should be evaluated and addressed by a designated industry consensus organization charged with reviewing network management practices. In the meantime, a moratorium on the use of RST Injections for purposes of network management is appropriate.

---

<sup>19</sup> See Mail Carrier Charged With Theft of Gift Cards, The Associated Press (Nov. 27, 2009), available at <[http://www.northjersey.com/news/crime\\_courts/crime\\_courts\\_news/75534477.html](http://www.northjersey.com/news/crime_courts/crime_courts_news/75534477.html)>.

<sup>20</sup> This is not to suggest that RST Injection might not have some national security or law enforcement purpose or that it should be banned altogether, but rather that it should not fall within the penumbra of “reasonable network management.”

<sup>21</sup> See Sally Floyd, “Inappropriate TCP Resets Considered Harmful,” Internet RFC 2260 (Aug. 2002), available at <<http://www.ietf.org/rfc/rfc3360.txt?number=3360>>.

**C. “Prevent the Transfer of Unlawful Content” and “Prevent the Unlawful Transfer of [Lawful] Content”**

The third and fourth prongs of the Commission’s definition of “reasonable network management” provide that IAPs may manage network traffic to “prevent the transfer of unlawful content” and “prevent the unlawful transfer of [lawful] content.” NPRM ¶ 135.

While a narrow exception to any non-discrimination rules to address the needs of law enforcement officials may be prudent, the NPRM’s discussion of reasonable network management improperly suggests that law enforcement considerations should separately enter into the analysis of whether a network management practice is reasonable. The FCC should neither mandate nor encourage IAPs proactively to intercede in civil or criminal matters by blocking or filtering speech, whether in relation to “reasonable network management” or otherwise. There are inescapable problems with this approach which deputizes IAPs into “content police.” The Commission is not the appropriate federal agency to establish, in the first instance, which content is “lawful,” or delegate to a private party the responsibility of doing so.

Fortunately, this problem is avoidable. The NPRM states (¶ 133) that the rules should be subject to “(1) reasonable network management, (2) the needs of law enforcement, and (3) the needs of public safety and homeland and national security.” (Discussed *infra* III.D.) Each qualification is appropriate, and by ensuring that each of these considerations remains separate from the other the Commission can avoid deputizing IAPs.

As explained below, the Final Rule should not conflate law enforcement issues with network maintenance. The following sections explain that: (a) law enforcement and civil dispute adjudication are not relevant to “reasonable network management” because the NPRM is limited in application to lawful content, services, and applications; (b) even assuming law enforcement were relevant, law enforcement is not network management; and (c) deputizing network operators is bad

policy and quite likely unconstitutional. Section III.C.4 concludes with recommended modifications to the rule that would remedy this problem.

**1. Because the first five principles as articulated in the NPRM are limited to lawful conduct, the question of law enforcement and civil dispute adjudication is not relevant to “reasonable network management.”**

Each of the five substantive principles is limited to content, services, and applications that are lawful. NPRM ¶ 92. Accordingly, unlawful content, services, and applications are subject neither to these rules nor the exception for reasonable network management. IAPs are not prevented by the NPRM from discriminating against unlawful content services or applications, because the NPRM does not extend to them. If a broadband provider is advised by law enforcement officials or the National Center for Missing and Exploiting Children (NCMEC) that particular files constitute child pornography, for example, the NPRM does not circumscribe how the broadband provider treats that content — it is simply unlawful. NPRM ¶ 139. Treating that content differently does not constitute “reasonable network management,” however. Blocking such content would be discriminatory under any definition of that word. This discrimination is beyond the scope of the NPRM, however, because the NPRM’s non-discrimination policy does not extend to unlawful content. Stated otherwise, non-discrimination is the rule; lawfulness is the scope of the rule; “reasonable network management” is an exception to the rule.

Conversely, this means that IAPs will only be invoking this exception with respect to lawful content, services, and applications. Each and every time a broadband provider engages in “reasonable network management,” therefore, it will be restricting lawful transmissions of lawful content. There are therefore considerable First Amendment implications to a broad invitation by the FCC for IAPs to judge the relative merits of legal content.

**2. Even if unlawful content, services, and applications were germane to the NPRM, law enforcement is not network management.**

Even if the five substantive rules were not circumscribed so as to address only lawful content, services, and applications, law enforcement activities do not fit within any definition of “network management.” IAPs have consistently claimed that ‘network management’ (reasonable or otherwise) involves engineering decisions. Having taken the position that network management entails “engineering decisions,” network operators cannot now claim that legal decisions made by lawyers regarding the adjudication of legal disputes, legal compliance, content evaluation, or law enforcement assistance are “reasonable network management.” Network management must be motivated by engineering concerns, not legal or business concerns.

Undoubtedly, calls may be made for using “reasonable network management” as a vehicle for vindicating social interests unrelated to the sound operation of broadband networks. The fact that increased broadband access may assist in achieving social policy goals does not mean, however, that social policy goals should in turn be shoehorned into what constitutes “reasonable network management.” The Commission should reject appeals to shift the focus of network management from the welfare of the network and its subscribers to the welfare of the public. The FCC, not individual IAPs, is charged with ascertaining and promoting the “public interest.” IAPs are not equipped, nor should they be empowered, to be the private arbiters of the relative merits of a given data packet in pursuit of abstract social interests.

**3. Conflating network management with the adjudication of civil disputes and criminal matters would usurp the role of the federal judiciary and constitutes bad policy.**

The ease with which socially significant speech can be alleged to be unlawful indicates the danger of elevating IAPs into the position of gatekeepers of contested speech. IAPs are poorly equipped to supplant or supplement the activities of law enforcement officials and the

judiciary by adjudicating the merits of unresolved criminal or civil disputes surrounding content, services, and applications. As stated previously, this issue is irrelevant to the NPRM, because the NPRM does not extend to unlawful activities. By suggesting that “reasonable network management” extends to policing content, however, the Commission creates the inevitable risk that it will be forced to assess how much lawful content a broadband provider can block in pursuit of general law enforcement.

While in a few narrow areas of law, such as child pornography, a visual inspection of individual elements of content may tend to establish a *prima facie* showing that content is unlawful, in almost all other cases IAPs will lack essential facts for determining the lawfulness of acts, content, services, and applications, as well as the authority to make such a determination unilaterally.

Rather than empowering IAPs to block traffic that merely appears to be unlawful, the Commission should implement regulations that protect IAPs from liability and make clear that IAPs are not obligated to search for and block potentially unlawful content absent a directive from a court of competent jurisdiction or law enforcement authority. On the other hand, IAPs that engage in the blocking of content that is ultimately deemed to be lawful content should face liability from the parties who have been damaged. Importantly, the Commission should not lose sight of the fact that once content has been blocked, a consumer may be irreparably harmed. If a subscriber needs access to lawful content or a political candidate needs to disseminate an important message on a time-sensitive basis, yet that traffic is wrongfully blocked by an IAP, the public may suffer irreversible harm — be it the loss of a business deal or the inability to influence the political process. In all cases, the Commission should avoid empowering IAPs, who may have various and conflicting reasons to desire to block traffic, from restricting the public’s freedom of speech.

#### 4. Recommendations for Final Rule

In light of the foregoing, CCIA recommends the following in the context of the Commission's definition of "reasonable network management" (NPRM ¶ 135):

- a) ***The definition should not confuse "allegedly unlawful" and "unlawful."***

Because the scope of the non-discrimination rule is defined in reference to lawfulness, it is essential that the final rule should make clear that "unlawful" does not mean "allegedly unlawful." NPRM ¶ 135. The spirit of the NPRM would be eviscerated if content, services, and applications were, based on the mere allegation that they were 'unlawful,' guilty and thus subject to discrimination until proven innocent. Nor does the First Amendment countenance the creation of a regime that exculpates discrimination against lawful speech because the discrimination serves the purportedly higher purpose of preventing unlawful speech (much less, lawful speech transmitted in an unlawful manner).

The argument, in essence, is that protected speech may be banned as a means to ban unprotected speech. This analysis turns the First Amendment upside down. The Government may not suppress lawful speech as the means to suppress unlawful speech. Protected speech does not become unprotected merely because it resembles the latter.

*Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 255 (2002).

The Commission should not do indirectly what the Supreme Court has held it cannot do directly. Absent clear standards by which an IAP can establish conclusively that certain content is unlawful — not that it appears to be unlawful — the Commission should not condone any IAPs' blocking of the transmission of traffic.

In addition to constitutional concerns, the dangers of a guilty-until-proven-innocent approach are not academic. Flawed allegations that speech is unlawful are not uncommon.

Research on the use and misuse of DMCA safe harbors, for example, found that “[o]ver half – 57% – of notices sent to Google to demand removal of links in the index were sent by businesses targeting apparent competitors.” Similarly, efforts to silence political speech through misrepresentations about lawfulness are not unknown to federal courts.

IAPs are not courts of law, and with the exception of content that tends to be facially unlawful (such as child pornography), IAPs will be incapable of determining whether speech or applications would be ruled as lawful or unlawful. Content, services, and applications alleged to be unlawful by interested parties (either under U.S. law or under the law of some foreign jurisdiction) should be entitled to the same degree of protection as all other content, services, and applications. Accordingly, the Commission should define “unlawful” to refer to content, services, and applications that are adjudicated to be contrary to U.S. criminal law.

**b) *The definition should not confuse civil disputes and criminal law.***

“Unlawful” should be defined to mean “violating U.S. criminal law.” As IAPs are poorly equipped to adjudicate legal matters, they should not preside over and adjudicate civil disputes among private parties. Placing IAPs in the position of adjudicating the legal merits of indefinite and/or broad causes of action under state and federal law, including prohibitions against ‘unfair and deceptive’ conduct, defamation, libel, and copyright infringement without proper safeguards, is unwise and contrary to public policy.

**c) *The definition should not confuse the transfer of unlawful content with the unlawful transfer of lawful content.***

The NPRM wisely differentiates between unlawful content and the unlawful transfer of lawful content, *id.* ¶ 135, although as stated above, no reference to unlawfulness is necessary in a “reasonable network management” exception when the rule to which the exception applies deals only with lawful content, services, and applications. The NPRM erred, moreover, if

it intended to suggest that the unlawful transfer of lawful content makes the underlying content unlawful. *Id.* ¶ 16 (referring to “the transfer of unlawful content, such as the unlawful distribution of copyrighted works.”).

The vast majority of content transferred unlawfully via broadband networks is lawful content. An unauthorized reproduction of a Hollywood film is not itself unlawful. With a few narrow exceptions, Congress cannot constitutionally prohibit the possession of such a film. For example, some Hollywood films may be “unlawful” in the People’s Republic China. In the United States, however, even an unauthorized reproduction of a Hollywood film, once made, is not itself “unlawful.” Rather, the act of reproducing the film was unlawful if that act violated one of the exact “bundle of rights” granted by Congress to the rightsholder via 17 U.S.C. § 106. Further performances or displays of the unauthorized reproduction may violate this limited government-granted monopoly if the individual is “using or authorizing the use of the copyrighted work in one of the five ways set forth in the statute.” *See Dowling v. United States*, 473 U.S. 207, 217 (1985). Prohibiting content itself, however, is largely beyond the reach of Congress.

To avoid conflating unlawful content with the unlawful transfer of lawful content, one must differentiate the unlawfulness of an act (the unlawful transfer) from the unlawfulness of content itself. *Free Speech Coalition, supra*, 535 U.S. at 253 (“to protect speech for its own sake, the Court’s First Amendment cases draw vital distinctions between words and deeds”). Just as possessing alcohol is legal while distributing it to minors is not, the Copyright Act’s prohibitions are delineated by verbs, not nouns. *See Dowling, supra*.

The most appropriate manner for addressing this problem is to strike from the definition of “reasonable network management” the elements stating: “(iii) prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content.” NPRM ¶ 135. Because the

NPRM applies only to lawful activities, the quoted elements of the definition would only be invoked with respect to lawful content. They should therefore be struck to avoid First Amendment obstacles. If it is only unlawful content at issue, on the other hand, then the language is surplusage and should be struck in any event.

To the extent the Commission deems it necessary to address unlawful content, however, the final rule should differentiate between unlawful content and lawful content whose transmission may be unlawful (or merely “unauthorized,” which is not legally equivalent to unlawful). With respect to the primary category of “lawful content, unlawfully transmitted” identified in the NPRM — copyright infringement — Congress has already established how IAPs are to prevent the unlawful transfer of content: through compliance with Section 512 of the Digital Millennium Copyright Act. 17 U.S.C. § 512. Congress carefully balanced various competing interests in crafting this provision; that balance should not be readjusted through a regulatory process. Indeed, previous efforts by the Commission to re-apportion responsibilities under federal copyright law have not ended fruitfully. *See American Library Ass’n v. FCC*, 406 F.3d 689, 704 (D.C. Cir. 2005) (rejecting as “strained and implausible” efforts to find a jurisdictional home for an order mandating that industry undertake certain obligations to protect technology).

- d) *The final rule should state that the antidiscrimination rules are subject to the needs of law enforcement officials, rather than the more amorphous “law enforcement.”***

The Commission could lessen the risk of accidentally deputizing network operators into *ad hoc* law enforcement vigilantes by clarifying that non-discrimination rules should be subject to the needs of law enforcement officials. The present reference to “law enforcement” (NPRM ¶ 133) could be broadly misconstrued, and should not be understood to apply to any user or provider who purports to enforce a third party’s compliance with a civil legal obligation. Had

Congress intended to deputize IAPs to be proactive private enforcers of state and federal law, it could have done so via CALEA. As Congress opted against such an approach, so too should the Commission in this proceeding.

**D. Addressing Law Enforcement, Public Safety, and Homeland and National Security Concerns**

Appropriately, the Commission has also recognized that law enforcement, public safety and homeland and national security interests could necessitate that an IAP temporarily adjust its network management practices in order to prioritize certain traffic or prevent or intercept the transmission of certain content.<sup>22</sup> By definition, these actions fall outside the categories of routine network management and involve specialized content and/or network traffic intervention.

Specifically, the Commission has proposed to adopt two rules:

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.<sup>23</sup>

Nothing in this part supersedes any obligation of a provider of broadband Internet access service may have — or limits its ability — to deliver emergency communications, or to address the needs of public safety or national or homeland security authorities, consistent with applicable law.<sup>24</sup>

CCIA wholly agrees with the Commission that law enforcement and national security concerns would justify disrupting business as usual on the Internet during a period of local, state, or national emergency or to respond to the needs of law enforcement. Again, however, CCIA respectfully suggests that the Commission answer the important question, “Who decides?”

---

<sup>22</sup> NPRM ¶¶ 142-147.

<sup>23</sup> *Id.* ¶ 143.

<sup>24</sup> *Id.* ¶ 146.

In other words, who decides when there is a national emergency? Who decides when law enforcement needs should permit someone's Internet transmissions to be intercepted? CCIA respectfully submits that the answer to these questions is, in both cases, that neither the Commission nor the IAPs should have that power. Rather, the agency or individual with proper statutory authority (in the case of a local, state, or national emergency) or a court of competent jurisdiction (through the issuance of a search warrant) should be required to take action before broadband access to a particular individual, in a particular region, or the nation is altered.<sup>25</sup>

Moreover, when it comes to an IAP assisting law enforcement in the execution of its duties, the Commission should ensure that its rules do not conflict with constitutional requirements imposed upon law enforcement personnel. Namely, the Commission should be cautious about condoning or implying that an invasion of privacy is appropriate merely because law enforcement has suggested the information could be useful to a legal investigation. Current law requires a search warrant be issued by a court of competent jurisdiction before computers and email may be searched, and that requirement should, indeed must, continue to apply.<sup>26</sup>

---

<sup>25</sup> For example, the National Emergencies Act provides that the President may declare national emergencies. *See* 50 U.S.C. § 1621(a) (“With respect to Acts of Congress authorizing the exercise, during the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency. Such proclamation shall immediately be transmitted to the Congress and published in the Federal Register.”). Moreover, Congress has been considering the Cybersecurity Act of 2009, S. 773, which was introduced by Senator Rockefeller. The Cybersecurity Act of 2009 provides that the President may “declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network.” *Id.* § 18(2). Accordingly, it is doubtful that the Commission or any individual IAP should take action to limit or shut down Internet traffic in the event of a perceived emergency, without the appropriate governmental entity taking legal action to declare a state of emergency.

<sup>26</sup> *See, e.g., United States v. Adjani*, 452 F.2d 1140 (9th Cir. 2006).

Accordingly, CCIA supports a Commission clarification that assistance to law enforcement must be “consistent with applicable law.”

In sum, CCIA would recommend that the intended impact of the proposed rules be clarified by removing the “or limits its ability” language in each of the proposed rules. This language may be inadvertently interpreted by IAPs to suggest that there is a degree of discretion that each IAP enjoys in deciding when to alter its network management practices in response to *perceived* emergencies or *perceived* law enforcement needs. Rather, IAPs should be prepared to meet declared emergencies and assist in law enforcement operations when appropriate safeguards have been met. Our nation’s system of checks and balances compels this conclusion.

Accordingly, CCIA respectfully suggests that the proposed rules be changed to read as follows:

Nothing in this part supersedes any obligation a provider of broadband Internet access service may have to address the needs of law enforcement acting in conformity with applicable law.

Nothing in this part supersedes any obligation of a provider of broadband Internet access service may have to deliver emergency communications, or to address the needs of public safety or national or homeland security authorities acting in conformity with applicable law.

These rules would strike an appropriate balance between subscriber autonomy and IAP/network operator authority.

#### **IV. NETWORK OPERATORS AND IAPs SHOULD BE REQUIRED TO PUBLISH ALL NETWORK MANAGEMENT PRACTICES, TERMS OF SERVICE, AND RESTRICTIONS CLEARLY AND CONSPICUOUSLY TO CONSUMERS**

The Commission has proposed the adoption of a sixth network neutrality principle of transparency. Specifically, the Commission has proposed adopting the following rule:

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.<sup>27</sup>

In the NPRM, the Commission seeks comment regarding “what consumers need to know about network management practices to make informed purchasing decisions and to make informed use of the service they purchase.”<sup>28</sup> The Commission also seeks comment regarding “how this information should be disclosed to users”<sup>29</sup> and “what information is currently available, what additional information should be made available, and how this information should be made available to content, application, and service providers.”<sup>30</sup>

CCIA applauds the Commission for its efforts to promote consumer confidence by fostering greater transparency. CCIA believes that disclosure to consumers is an important tool in the Commission’s arsenal as it seeks to maintain and reinforce network neutrality that has proven to be so vital to the Internet’s evolution. Indeed, the Justice Department links disclosure requirements to “the *quality* of competition” in Internet access service.<sup>31</sup> It has provided the Commission with examples in other countries, including Ireland and the United Kingdom, where broadband-specific consumer information tools, such as price comparisons, are already in place.<sup>32</sup> Such transparency rules require caution, however: the Justice Department advised that “the

---

<sup>27</sup> NPRM ¶ 119.

<sup>28</sup> *Id.* ¶ 125.

<sup>29</sup> *Id.* ¶ 126.

<sup>30</sup> *Id.*

<sup>31</sup> “One attractive policy alternative for the Commission is to seek to improve the *quality* of competition by ensuring that consumers get better information about their choices, so that they can compare offers and select the broadband service that best suits their needs.” DOJ *Ex Parte* at 25 (emphasis in original).

<sup>32</sup> DOJ *Ex Parte* at 26-27.

Commission should take care to ensure that it does not facilitate price collusion or limit the ability of providers to compete on price.”<sup>33</sup>

However, CCIA also agrees with other commenters that disclosure alone is not enough.<sup>34</sup> Because the last-mile Internet access market is primarily a duopoly or oligopoly, at best, the Commission must continue to promote competition and must recognize that IAPs will have a degree of market power that may restrict consumers’ ability to switch IAPs, even in the face of unreasonable — though not necessarily anticompetitive — network management practices.

CCIA submits that the Commission’s transparency requirements, already qualified by the need to disclose information only to the extent reasonably required by users, need not be further qualified by the “subject to reasonable network management” language. CCIA can think of no situation where reasonable network management practices would dictate that an IAP’s network management practices need not be disclosed. In other words, CCIA understands that IAPs may desire to limit the information disclosed because of confidentiality and business concerns, and CCIA understands that IAPs may need to limit the disclosure of information based on legitimate national security or law enforcement needs, but it can envision no situation where reasonable network management practices, as defined in the Commission’s proposed definition, should enable an IAP to prevent disclosing the network management practices it actually employs on a routine basis. Accordingly, CCIA would urge the Commission to modify the proposed sixth transparency principle to read as follows:

Subject to the express needs of law enforcement, public safety, and homeland and national security, a provider of broadband Internet access service must disclose such information concerning network

---

<sup>33</sup> DOJ *Ex Parte* at 27.

<sup>34</sup> See van Schewick Testimony at 4.

management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections specified in this part.

CCIA believes that standardization will be the key to providing subscribers with the knowledge necessary to make an informed decision regarding the selection of an IAP. CCIA would encourage the Commission to combine the data that will be acquired through the recently released and anticipated state-based broadband mapping grants with the data that IAPs will be required to produce under the transparency principle. In other words, to be most effective, a consumer should be able to identify with ease the following information — some of which would be acquired through the broadband mapping grants and other parts of which should be required disclosures of IAPs:

- (1) which IAPs serve his/her community;
- (2) the advertised download/upload speeds from each provider;
- (3) the amount of time the average user experiences speeds slower than the advertised download/upload speeds;
- (4) the minimum speed that the IAP contracts to provide to the consumer under each pricing plan, including any usage-sensitive or time-and-usage sensitive plans;
- (5) the manner in which the IAP prioritizes certain types of traffic, if at all;
- (6) the ability of subscribers to customize the manner in which their traffic will be prioritized;
- (7) any programs or services that the IAP blocks or degrades and, if degraded, the extent of the degradation that occurs;
- (8) any early termination fees or minimum contract periods that the IAP may include in its contract;
- (9) whether the IAP uses DPI technology and, if so, the reasons for and the limits of the use of DPI technology; and
- (10) the extent to which a subscriber can anticipate or expect privacy when using that IAP's broadband service.

CCIA would recommend that, though the Commission may desire to collect more exacting information from IAPs, a subscriber-friendly scale be created for most of these areas that could be easily reviewed by a consumer or business seeking to choose between IAPs. This information, together with the broadband maps, should be displayed on a website that is easy to find and navigate and is regularly updated. Links in the website could then direct subscribers to the more detailed contract terms and other information which each IAP should be required to post on their respective websites.

As it has done in the previous discussion regarding network management, CCIA also urges the Commission to designate a dedicated technical advisory group to be the initial arbiter of how much and what information must be disclosed by IAPs in order to enable users to enjoy the protections envisioned by the Commission. The industry should have a significant voice in the establishment of these disclosure standards, and the Commission can obtain more certainty, while also preserving greater flexibility to respond to technological innovations, by inviting the participation of industry experts to evaluate these issues.

**V. THE COMMISSION SHOULD ESTABLISH AN ADVISORY PANEL AS THE TRIBUNAL OF FIRST RESORT FOR THE ENFORCEMENT OF ANY NEW RULES OR GUIDELINES**

The Commission seeks comment on whether it “should adopt procedural rules specifically governing complaints involving alleged violations of any Internet principles we codify in our regulations.” NPRM ¶ 176. The Commission’s first inclination, it appears, is to enable complainants to pursue relief at the Enforcement Bureau under some type of Section 208 procedure. *See id.* ¶ 175. CCIA would like to suggest an alternative approach that would authorize a dedicated multidisciplinary technical advisory group to consider complaints regarding

Internet access in the first instance, preserving Enforcement Bureau resources for the review, and possible adoption of, the panel's recommendations.

The complaint procedures that the Enforcement Bureau presently employs are not well suited to the types of disputes likely to arise from the open access rules adopted in this proceeding. Adjudicatory cases before the Enforcement Bureau increasingly resemble full-scale civil trials, including the exchange of discovery, testimony, and expert reports. As such, such cases require a year or more to be resolved and require a considerable investment of the litigants' and the Commission's resources.<sup>35</sup> Disputes under the forthcoming open access rules, by contrast, are likely to arise from a comparatively smaller set of facts and have a comparatively more narrow scope than the Enforcement Bureau presently handles. Moreover, open access disputes are likely to focus more closely on the operation of network management software than on transmission facilities, and thus the Enforcement Bureau may have less expertise in these disputes than it has for typical common carrier complaints.

The Commission already is considering in this proceeding whether to establish, via the Office of Engineering and Technology ("OET"), a "technical advisory process" in order to attain "a thorough understanding of current technology and future technological trends." NPRM ¶ 177. The Commission's goal is that OET "will create an inclusive, open, and transparent process

---

<sup>35</sup> By way of example, the *Comcast Network Management Practices Order* arose from the formal complaint of Free Press and Public Knowledge against Comcast filed on November 1, 2007, regarding Comcast's practice of blocking bit-torrent uploads. The Commission released its order in that matter on August 20, 2008, nearly ten months after the formal complaint was filed. The *Comcast Network Management Practices Order* has been appealed, however, to the United States Court of Appeals for the District of Columbia Circuit and oral argument was heard on January 8, 2010. See *Comcast Corporation v. FCC*, No. 08-1291 (D.C. Cir.). As such, more than two years after the formal complaint was filed, it is still unclear whether the FCC has ever provided any lawful and enforceable guidance regarding the outer limits of "reasonable network management practices." This sort of prolonged uncertainty would seem to compromise the Commission's stated objective of fostering innovation.

for obtaining the best technical advice and information from a broad range of engineers.” *Id.* This type of advisory body is equally appropriate for enforcing the rules adopted in this proceeding.

CCIA suggests that a similar panel be established and authorized to act as the tribunal of first resort for disputes regarding open Internet access. This panel should include representatives of the telecommunications, equipment, software application, and website development industries as well as independent consumer advocacy and policy consulting organizations. As Chairman Genachowski stated at the recent GigaOM event, amassing the expertise of these various sectors may produce the most efficient regime for preserving an Open Internet.<sup>36</sup>

As a solution for the near term, CCIA encourages the Commission to designate an existing entity, such as the IETF, or establish a new technical advisory panel that will consider and evaluate disputes over network management practices in the first instance. This entity should be empowered to provide clear guidance to IAPs, such that the IAPs are not left wandering the darkness waiting for the Commission to complete case-by-case adjudications. The industry will benefit from an understanding of what practices are presumptively deemed reasonable, and what practices are presumptively unreasonable. To the extent that there are practices that fall in the middle of the spectrum, the technical advisory entity, rather than the Commission’s adjudicatory process, should be the first place to which complainants go to seek review. This process will preserve the Commission’s resources, prevent unnecessary delay, and allow greater industry input into the process.

---

<sup>36</sup> Livestream video of event available at <[http://gigaom.com/2010/01/06/livestream-fcc-chairman-julius-genachowski-on-broadband-policy/?utm\\_source=twitterfeed&utm\\_medium=twitter](http://gigaom.com/2010/01/06/livestream-fcc-chairman-julius-genachowski-on-broadband-policy/?utm_source=twitterfeed&utm_medium=twitter)> (Jan. 6, 2010).

An example of independent telecommunications management is Neustar, the Administrator of the North American Numbering Plan. The Commission has authorized Neustar, a private corporation, to conduct audits of whether numbering resources are being used and to reclaim unused numbers. *See* 47 C.F.R. § 52.13. It is required to be “an independent and impartial non-governmental entity.” *Id.* Neustar is the first arbiter of whether numbering resources are being used appropriately; the Enforcement Bureau oversees, reviews, and enforces Neustar’s findings. *Id.* § 52.19(k). This type of delegation is not ideally suited to open access disputes, however, because of the lack of quick turnaround capability and direct FCC oversight. CCIA therefore recommends that the tribunal of first resort should be a panel comprised of expert representatives from the telecommunications, application, web hosting and development, and content industries, and the Commission itself.

With regard to standard of review, the Commission has proposed that it abandon the standard adopted in the *Comcast Network Management Practices Order* by which a network management practice would be judged. NPRM ¶ 137. In the *Comcast Network Management Practices Order*, the Commission held that a network management practice would be considered “reasonable” if it “further[ed] a critically important interest and [is] narrowly or carefully tailored to serve that interest.”<sup>37</sup>

CCIA believes that the Commission adopted the appropriate standard in the *Comcast Network Management Practices Order* but suggests that the exacting standard employed in that case may not be necessary in all cases. Strict liability need not be applied to all network management disputes. Rather, a negligence standard is an appropriate means to address malfeasance appropriately and to deter further misconduct. Thus, a failure to comport with the

---

<sup>37</sup> *Comcast Network Management Practices Order*, 23 FCC Rcd. at 13055-56, ¶ 47.

network management practices adopted in this proceeding, if they harmed a subscriber, other IAP, or a content provider and has no nexus to a cognizable network harm, would result in liability even absent any evidence of discriminatory motive or intent. Further, any IAP action not reasonably tailored to address that cognizable network harm should likewise incur liability. The Commission should be emphatic, however, in stating that network management practices having a plainly anticompetitive, unjustified purpose will not be tolerated, nor will the use of network management practices as a subterfuge for ignoring or overriding unharmed consumer choices.

### **CONCLUSION**

CCIA applauds the Commission for initiating this proceeding, and is confident that the rules the Commission will adopt will ensure a procompetitive and robust environment for Internet access while allowing network operators to maintain network security and the meaningful protection of intellectual property.

Dated: January 13, 2010

Respectfully submitted,

By: s/ Jonathan E. Canis  
Jonathan E. Canis  
Stephanie A. Joyce  
G. David Carter  
Arent Fox LLP  
1050 Connecticut Avenue, N.W.  
Washington, D.C. 20036  
Tel. (202) 857-6000  
Facsimile (202) 857-6395  
Email: Canis.Jonathan@arentfox.com  
Joyce.Stephanie@arentfox.com  
Carter.David@arentfox.com

*Counsel to CCIA*

Edward J. Black  
Catherine R. Sloan  
Matthew C. Schruers  
CCIA

900 17th Street, N.W.  
Suite 1100  
Washington, D.C. 20006  
Tel. (202) 783-0070  
Facsimile (202) 783-0534  
Email: EBlack@ccianet.org  
CSloan@ccianet.org  
MSchruers@ccianet.org